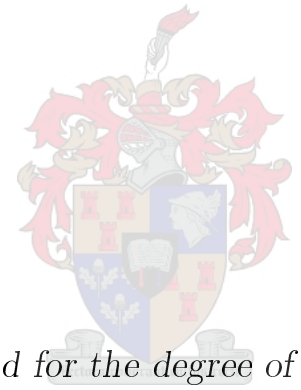
On contributions to the theory of Near-vector spaces and graphs thereof

by

Lesley Karin Wessels



Dissertation presented for the degree of Doctor of Philosophy in the Faculty of Science at Stellenbosch University

Supervisor: Dr. Karin-Therese Howell

Co-supervisor: Dr. Samantha Dorfling

December 2020

Declaration

By submitting this dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 2020/08/21 .....

Abstract

On contributions to the theory of Near-vector spaces and graphs thereof

L.K Wessels

Department of Mathematical Sciences, Division Mathematics
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Dissertation: PhD

December 2020

In this thesis, our aim is to add to the existing body of work on near-vector spaces and their representation using graphs. We introduce two new graphs for constructions of near-vector spaces using finite fields, the fibration and subspace inclusion graph and study their properties. As a second focus, we look at the quotient spaces of a near-vector space, where some of the maximal regular subspaces have been factored out. For construction of near-vector spaces from copies of finite fields, we completely characterise regularity, describe the quasi-kernel and some of its graphs. We conclude with some reconstruction problems for the near-vector space graphs introduced and one related to finite near-fields.

Uittreksel

Oor die bydraes tot die teorie van naby-vektorruimtes en grafieke daarvan

L.K Wessels

Departement Wiskundige Wetenskappe, Afdeling Wiskunde
Universiteit van Stellenbosch,
Privaatsak X1, Matieland 7602, Suid Afrika.

Proefskrif: PhD

Desember 2020

In hierdie tesis, beoog ons om by te dra tot die bestaande werke oor naby-vektorruimtes en hul voorstelling met behulp van grafieke. Ons stel twee nuwe grafieke voor, naamlik die fibrasie- en die deelruimte-insluiting grafiek, vir naby-vektorruimters wat van kopieë van eindige liggame gebou is, en bestudeer hul eienskappe. 'n Tweede fokuspunt wat ons beskou is die kwosiëntruimte van 'n naby-vektorruimte, waar ons sekere van die maksimale regulêre deelruimtes uitfaktor. Naby-vektorruimtes wat vanuit kopieë van eindige liggame gebou is, word volledig gekenmerk deur middel van regulêriteit, ons beskryf die kwasie-kern sowel as sekere van hul grafieke. Ons sluit af met 'n paar rekonstruksie probleme van naby-vektorruimte grafieke wat voorgestel was, asook een wat verwant is aan eindige naby-liggame.

Acknowledgment

I have had the priviledge to have had some of the most amazing role models in my life, starting with my supervisor, Dr Karin-Therese Howell. I would like to convey my immense gratitude to her for her guidance and unwaivering support. I would not be where I am today were it not for her constant care, efforts and understanding.

It was a priviledge and a pleasure to meet and study under Dr Samantha Dorfling. I thank her for hosting me in the Mathematics department at the University of the Free State. I extend my thanks to her colleagues in the department for making me feel welcome. I thank Prof Philippe Cara for his invaluable input to, and support of, my work. I thank the Dorfling-Cara family, including Janine, for making my stay in Bloemfontein a pleasant one.

I thank Sogo Sanon, Prudence Djagba and Jacques Rabie for their valuable input.

My heartfelt thanks to my friend and mentor, Prof Marina Rautenbach, who constantly encouraged me to find what I'm passionate about and to follow my own path. She inspires me every day.

I thank Prof Ingrid Rewitzky, our current head of department, for all of her support through the years, and especially for her constant encouragement and belief that I am capable of seeing this degree through to the end. She has been someone with whom I could share matters of the soul with, and I am immensely grateful for that.

I have had many friends throughout my life who have inspired me, and none moreso than Greg Newman. His academic path alone has inspired me to be less complacent. He will forever be the Mal to my Zoë.

I thank the department of Mathematics, as well as the Science faculty, for bearing the financial burden of my studies. While I completed my degree as a staff member, I have received financial assistance from the National Research Foundation of South Africa in past attempts at obtaining my degree. I am most grateful for the support that I was granted.

Thank you, Retha, Ilse, Doret, Bruce, Gareth, Karin, Lauretta, Lisa, Vanessa and especially Arnold and Mark. You inspire me every day to be a better version of myself. I am a better person for knowing all of you.

I thank every colleague in our department, past and present, who has made our department the happy place that it has been for me. I especially thank Proff Barry Green and Florian Breuer.

I thank my entire Anglican family, especially the ones that I have belonged to as a member. I thank the Williams family, especially, as my second family. I thank every priest who has every taken the time outside of mass to discuss issues of interest to me.

I thank my family, the Wessels, Forbes and Hendricks clans, for their undying support. I hope that I have made you proud. I love every one of you.

I count every person above as a blessing in my life.

Last but not least, I thank God, the Holy Trinity, for carrying me through every moment that I've spent on this earth. I love You more every day.

Dedications

To George and Cecilia Wessels

Contents

Chapter 1

Introduction

The concept of a near-field was first introduced in 1905 by an American mathematician named Leonard Dickson in [10]. In general, any division ring (including any field) is a near-field. Dickson modified the multiplication of a finite field, while leaving the addition unchanged. In doing so, he produced the first known examples of near-fields that were not division rings. These near-fields are called Dickson near-fields.

Geometry was the main motivator for modern near-field theory. For further reading, see [29] on weak affine spaces, [25] on projective incidence groups and [3] on parallel structures. Near-fields have applications in projective geometries, as well. In 1943 the American mathematician Marshall Hall published a paper on projective planes, wherein he constructed a family of non-Desarguesian projective planes known today as Hall planes [13]. He defined the smallest such plane of order nine, from the Dickson near-field of the same order. Near-fields are also important in near-vector space theory. In [30], van der Walt proved that every finite dimensional near-vector space can be characterised in terms of a finite number of near-fields.

Near-vector spaces have less linearity than traditional vector spaces. A few authors have tried to capture this. In [5] Beidleman defined a near-vector space in terms of near-ring modules, while in [24] Karzel defined a near-vector space in terms of a group (not necessarily commutative) and a double loop. Subsequently in 1974 André [4] defined a third notion of a near-vector space. These have been extensively studied. In this thesis our focus will be on these near-vector spaces.

In 2010 Howell and Meyer characterised all finite dimensional near-vector spaces over $\mathbb{Z}_p$, for p a prime [19] and then extended these results to all finite dimensional near-vector spaces constructed from finite fields [20]. The subspaces of near-vector spaces of various constructions, ranging from those closest to traditional near-vector spaces to those further away, in terms of their quasi-kernel and regularity were studied in 2015 by Howell ([16]). In 2016, Howell and Boykett looked at the automorphisms of finite Dickson near-fields and

their application in finite-dimensional near-vector spaces constructed from finite Dickson near-fields.

In 2017, Rodtes and Chomjun [27] provided a new characterisation of isomorphic near-vector spaces determined by finite fields and gave a formula for counting the number of these spaces (up to isomorphism).

In 2018, Dorfling, Howell and Sanon looked at the decomposition of certain classes of finite-dimensional near-vector spaces and derived a formula for calculating the cardinality of the quasi-kernel. They also defined a regularity graph, which can be associated with each near-vector space. In [21], Howell and Sanon studied the linear and affine mappings of near-vector spaces while more recently, Howell, Chistyakov and Sanon gave the general form of finite-dimensional near-vector spaces constructed using finite fields, and studied their representation theory ([7]).

The aim of this thesis is to contribute to the existing body of work on near-vector spaces.

We begin in chapter two with the preliminary material we will need for our results. The material is divided into three sections, namely finite near-fields, near-vector spaces and graph theory.

Chapter three focuses on graphs and constructions of near-vector spaces. We begin by reviewing and adding a few new results to the regularity graph and then define and study two new graphs, the fibration graph and subspace inclusion graph. The fibers of a near-vector space are exactly the orbits of the action of the scalars on the additive group. Thus the fibration graph gives a graphical representation of these orbits. We study the fibration graph of finite-dimensional near-vector spaces constructed using finite fields, including its definition, some properties, when it is isomorphic to the regularity graph and for constructions using $\mathbb{Z}_p$, we give the complete description of the fibers. We also define a covariant functor between the category of finite graphs and the category of finite-dimensional near-vector spaces constructed from finite fields. This functor assigns to every finite-dimensional near-vector space its fibration graph. We show the functor is faithful, but not full and essentially surjective.

In [8] the subspace inclusion graph was defined for vector spaces. It graphically captures the containment of the subspaces of a vector space. We define the subspace inclusion graph of finite-dimensional near-vector spaces constructed using copies of finite fields, study its order, derive some properties and a formula for calculating the degree of any vertex in the graph.

As part of the constructions, we look at direct sums of subspaces of near-vector spaces, as well as quotient spaces. Quotient spaces for near-vector spaces have not been studied

before, so this is an important contribution to the theory. We study the quotient space of a near-vector space formed by factoring some maximal regular subspaces in detail. For constructions using copies of finite fields, we completely characterise regularity, describe the quasi-kernel and give the fibration and regularity graphs. This material has been compiled into a first paper, "The quotient spaces of Near-vector spaces", co-authored with my supervisor and Professor P. Cara (Vrije Universiteit, Belgium) that has been submitted for publication. A second paper on the fibration and subspace inclusion graphs of near-vector spaces constructed using copies of finite fields and some reconstruction problems will follow.

Chapter four includes the application of a well-known problem in graph theory, called the reconstruction problem to algebra. We chose to look at three specific reconstruction problems involving near-vector spaces. The first is the reconstruction of near-vector spaces (up to isomorphism) given the fibrations, where one fiber has been removed from each fibration. The second problem involves the reconstruction of a near-vector space, given a fibration graph. The third and final problem involves a given graph with given order, and the reconstruction of a finite Dickson near-field from it.

I believe the biggest contributions that I've made is in defining and studying the subspace inclusion graph for near-vector spaces. I've learned that this graph may have some relevance to research done in incidence geometry. I feel that the characterisation of the fibres are a significant contribution as well. Lastly, the importance of quotient spaces in vector space theory illustrates the significance of the quotient near-vector spaces work. I value the contributions I made to this body of work.

Chapter 2

Preliminary material

In this chapter we give some preliminary material required for later chapters. There are three subsections. The first is on finite Dickson near-fields, the second on near-vector spaces and the third is on the graph theory we will need.

2.1 Finite Dickson near-fields

As mentioned in the introduction, the concept of a near-field was first introduced in 1905 by an American mathematician named Leonard Dickson in [10]. Near-fields are important in near-vector space theory. In [30], van der Walt proved that every finite dimensional near-vector space can be characterised in terms of a finite number of near-fields.

We will start with the definition of a near-field.

Definition 2.1.1. *([26]) A near-field F is a set, together with two binary operations, addition and multiplication, written $(F, +, \cdot)$, with the following properties:*

(i) $(F, +)$ *is a group (not necessarily abelian);*

(ii) $(F, \cdot)$ *is a semi-group;*

(iii) $(n_1 + n_2) \cdot n_3 = n_1 \cdot n_3 + n_2 \cdot n_3$ *for all* $n_1, n_2, n_3 \in F$*;*

(iv) $(F \setminus \{0\}, \cdot)$ *is a group.*

This is the definition of a right near-field. Analogously, there exists the concept of a left near-field, which satisfies all the axioms, except (iii), where instead we have $n_1 \cdot (n_2 + n_3) = n_1 \cdot n_2 + n_1 \cdot n_3$ for all $n_1, n_2, n_3 \in F$. By definition, near-fields are not required to be abelian. However, several authors have shown that the axioms of Definition 2.1.1 result in $(F, +)$ being abelian. It is clear that every field is a near-field. We will make use of right near-fields throughout this thesis. For more on near-fields we refer the reader to

[26]. From now on we will write ab instead of $a \cdot b$ to denote the product of a and b and S^* to denote $S \setminus \{0\}$ for any set S.

The following two subsets of a near-field will be important in our work. The first of these subsets, called the center of $(F, \cdot)$, contains all the elements of F which are commutative under multiplication. The second subset contains all the elements in F which satisfies the left distributive law. This subset of F is very useful for later results.

Definition 2.1.2. *([26]) Let F be a near-field.*
The center of $(F, \cdot)$ is defined as follows:

$$C(F) := \{x \in F : xy = yx, \ \forall y \in F\}.$$

The kernel of $(F, +)$ is defined as follows:

$$F_d := \{x \in F : x(y + z) = xy + xz, \ \forall y, z \in F\}$$

i.e., it is the set of distributive elements.

Proposition 2.1.3. *([26]) Let F be a near-field and F_d the set of all distributive elements. Then*

- *F_d is a division ring.*
- *F can be considered as a right vector space over F_d.*

The theory of finite Dickson near-fields rests on the existence of a pair of Dickson numbers, which we define next.

Definition 2.1.4. *([26]) For q and n in $\mathbb{N}$, (q, n) is called a pair of Dickson numbers if*

(a) q is some power p^l of a prime p;

(b) each prime divisor of n divides $q - 1$; and

(c) if $q \equiv 3 \pmod{n}$, then 4 does not divide n.

Example 2.1.5.

1. *The pair $(3, 2)$ is the smallest example of a pair of Dickson numbers to yield a proper finite Dickson near-field, as we will see.*
2. *Some more examples are $(5, 2), (4, 3), (5, 4), (5^2, 2), (5, 8), (p, 1)$, where p is a prime, to name but a few.*

$\Diamond$

For the purpose of constructing Dickson near-fields, we need to define what a coupling map is.

Definition 2.1.6. *([26]) A map*

$$\begin{array}{rcl} \phi : F^* & \to & Aut(F,+,\cdot) \\ n & \mapsto & \phi_n \end{array}$$

is called a coupling map, if for all $m, n \in F$,

$$\phi_n \circ \phi_m = \phi_{\phi_n(m)n}.$$

If ϕ is a coupling map on F, then we can define a new operation

$$m \circ_\phi n := \begin{cases} \phi_n(m)n & \text{if } n \neq 0 \\ 0 & \text{if } n = 0 \end{cases}$$

We give an example of a coupling map.

Example 2.1.7. *([26])*
The map $\phi : n \mapsto id_F$ is a coupling map on F. ◊

We can now express our near-field in terms of the new multiplication.

Proposition 2.1.8. *([26]) If ϕ is a coupling map on F, then $(F,+,\circ_\phi)$ is again a near-field.*

A Dickson near-field is defined in terms of this new multiplication.

Definition 2.1.9. *([26]) $(F,+,\circ_\phi)$ is called the ϕ-derivation of $(F,+,\cdot)$, denoted by F^ϕ. F is said to be a Dickson near-field if F is the ϕ-derivation of some field F.*

Before we show how to construct finite Dickson near-fields, the following from [26] tells us more about their distributive elements.

Theorem 2.1.10. *([26]) Let F be the $\phi-$derivation of the Galois field $GF(q,n) = GF(p^{ln})$, where (q,n) is a pair of Dickson numbers. Then*

$$C(F) = F_d = GF(q).$$

We now state the theorem that constructs a Dickson near-field from a given pair of Dickson numbers. We write $GF(q^n)^*$ to denote $GF(q^n) \setminus \{0\}$.

Theorem 2.1.11. *([26]) Let (q,n) be a pair of Dickson numbers and $GF(q^n)$ be the Galois field with q^n elements. Let β be a generator of $(GF(q^n)^*,\cdot)$ and let H be the subgroup of*

$(GF(q^n)^*, \cdot)$ generated by β^n.
Let α be the Frobenius-automorphism

$$f \to f^q$$

of $(GF(q^n), +, \cdot)$. Then $GF(q^n)^*/H$ can be represented as

$$\{H\beta, H\beta^{\frac{q^2-1}{q-1}}, \ldots, H\beta^{\frac{q^n-1}{q-1}} = H\}.$$

Let $\lambda(H\beta^{\frac{q^k-1}{q-1}}) := \alpha^k$, where $\alpha^k \in Aut(GF(q^n), +, \cdot)$. If

$$\pi : GF(q^n)^* \to GF(q^n)^*/H$$

is the canonical epimorphism, then $\phi = \lambda\pi$ is a coupling map on $GF(q^n)$ and

$$F = [GF(q^n)]^\phi = (GF(p^{ln}), +, \circ_\phi), \quad \text{where } q = p^l$$

is a near-field.

Remark 2.1.12.

- *All finite near-fields, excluding the 7 exceptional cases, are Dickson near-fields. (See [26]). We will exclude these 7 throughout this thesis.*
- *As remarked in [26], for a given Dickson pair (q, n), the Dickson near-field constructed using Theorem 2.1.11 is not unique and depends on the choice of the generator.*
- *In fact, there are $k = \dfrac{\varphi(n)}{i}$ non-isomorphic Dickson near-fields where φ is the Euler-function and i is the order of p mod n.*
- *We note that it is not difficult to prove that $\left\{ \dfrac{q^i - 1}{q - 1} \;\middle|\; 0 < i \leq n \right\}$ is a complete set of residues modulo n. (The proof is found in the Appendix A).*
- *By using the fact that $n \left| \left(\dfrac{q^n - 1}{q - 1} \right) \right.$ we can prove that $H\beta^{\frac{q^n-1}{q-1}} = H$.*

For a given pair of Dickson numbers, (q, n), we will denote a Dickson near-field associated with it by $DF(q, n)$. To illustrate this theorem, we give an example.

Example 2.1.13.
Consider the pair of Dickson numbers $(3, 2)$. Consider the Galois field $GF(3^2)$ with β a root of the polynomial $f(x) = x^2 + x + 2$ which is irreducible over $GF(3)$. It has elements

$$\{0, 1, 2, \beta, 2\beta, 1 + \beta, 1 + 2\beta, 2 + \beta, 2 + 2\beta\}.$$

$(GF(3^2)^*, \cdot)$ is cyclic and the above elements can be written as powers of β, with

$$GF(3^2)^* = \{\beta, \beta^2 = 2\beta + 1, \beta^3 = 2\beta + 2, \beta^4 = 2, \beta^5 = 2\beta, \beta^6 = \beta + 2, \beta^7 = \beta + 1, \beta^8 = 1\}.$$

H is the subgroup generated by β^2:

$$H = \{\beta^2, \beta^4, \beta^6, \beta^8\} = \{2\beta + 1, 2, \beta + 2, 1\}.$$

Then

$$\begin{array}{rcl} \alpha : GF(3^2) & \to & GF(3^2) \\ a & \mapsto & a^3 \end{array}$$

and

$$GF(3^2)^*/H = \{H\beta, H\beta^4\} = \{H\beta, H\}.$$

Note that $H\beta = \{\beta^3, \beta^5, \beta^7, \beta\} = \{2\beta + 2, 2\beta, \beta + 1, \beta\}$. Next we define the mappings λ and π to b:

$$\begin{array}{rcl} \lambda : GF(3^2)^*/H & \to & Aut(GF(3^2), +, \cdot) \\ H\beta^{\frac{3^k-1}{2}} & \mapsto & \alpha^k, \quad k \in \{1, 2\} \end{array}$$

and

$$\begin{array}{rcl} \pi : GF(3^2)^* & \to & GF(3^2)^*/H \\ b & \mapsto & Hb. \end{array}$$

This gives us our coupling map ϕ:

$$\phi = \lambda \circ \pi : GF(3^2)^* \to Aut(GF(3^2), +, \cdot).$$

Since ϕ is a coupling map on $GF(3^2)$, we have the following,

$$\begin{aligned} b \circ_\phi a &= \begin{cases} \phi_a(b)a & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases} \\ &= \begin{cases} ba & \text{if } a \in H \\ b^3 a & \text{if } a \notin H \\ 0 & \text{if } a = 0 \end{cases} \\ &= \begin{cases} ba & \text{if } a \text{ is a square} \\ b^3 a & \text{if } a \text{ is not a square} \\ 0 & \text{if } a = 0. \end{cases} \end{aligned}$$

$(DF(3, 2), +, \circ_\phi)$, with

$$x \circ_\phi y := \begin{cases} xy & \text{if } y \text{ is a square in } (GF(3^2), +, \cdot) \\ x^3 y & \text{otherwise} \end{cases}$$

gives the smallest Dickson near-field, which is not a field. In closing, we give the multiplication table for this new near-field:

$\circ_\phi$	0	β^2	$\beta^4=2$	β^6	$\beta^8=1$	β	β^3	β^5	β^7
0	0	0	0	0	0	0	0	0	0
β^2	0	β^4	β^6	1	β^2	β^7	β	β^3	β^5
$2=\beta^4$	0	β^6	1	β^2	β^4	β^5	β^7	β	β^3
β^6	0	1	β^2	β^4	β^6	β^3	β^5	β^7	β
$1=\beta^8$	0	β^2	β^4	β^6	1	β	β^3	β^5	β^7
β	0	β^3	β^5	β^7	β	β^4	β^6	1	β^2
β^3	0	β^5	β^7	β	β^3	β^2	β^4	β^6	1
β^5	0	β^7	β	β^3	β^5	1	β^2	β^4	β^6
β^7	0	β	β^3	β^5	β^7	β^6	1	β^2	β^4

By Theorem 2.1.10, $(DF(3,2))_d = GF(3) = \{0,1,2\}$. ◊

The following unpublished result was proved by P. Djagba and S.P. Sanon. We include the proof for completeness.

Theorem 2.1.14. *Let (q,n) be a pair of Dickson numbers. Let $GF(q^n)^* = \langle\beta\rangle$, $GF(q)^* = \langle\beta^i\rangle$ and $H = \langle\beta^n\rangle$. Then $(GF(q)^*,\cdot)$ is a subgroup of $(H,\cdot)$.*

Proof. Let β be a generator for $GF(q^n)^*$, and suppose that i is a positive integer such that $\langle\beta^i\rangle = GF(q)^*$. Since (q,n) is a pair of Dickson numbers, $H = H\beta^{\frac{q^n-1}{q-1}}$. Then we have that

$$1 = \beta^{i(q-1)},$$

and also that

$$1 = \beta^{q^n-1}.$$

This implies that

$$i(q-1) \equiv q^n - 1 \bmod (q^n-1)$$
$$i = k\left(\frac{q^n-1}{q-1}\right),$$

where $1 \leq k < q-1$ such that $gcd(k, q-1) = 1$. But

$$\beta^i = \beta^{k\frac{q^n-1}{q-1}} \in \langle\beta^{\frac{q^n-1}{q-1}}\rangle \subseteq H,$$

and hence $\langle\beta^i\rangle \subseteq H$. But $\langle\beta^i\rangle = GF(q)^*$, since β^i generates $GF(q)^*$ we have that $\langle\beta^i\rangle = GF(q)^*$ is a subgroup of H. □

By Theorem 2.1.11, H is a subgroup of $(\mathrm{GF}(q^n)^*,\cdot)$, but we have more:

Lemma 2.1.15. *([31]) Let (q, n) be a pair of Dickson numbers and $\circ_\phi$ the new multiplication. Then $(H, \circ_\phi)$ is a group.*

In fact by Theorem 2.1.14 and Lemma 2.1.15 we have that $(\mathrm{GF}(q)^*, \circ_\phi)$ is a subgroup of $(H, \circ_\phi)$.

According to Theorem 2.1.10 the order of $(DF(q,n))_d$ is q. This would mean that in the case where $q = p^l$ for l a positive integer, the centre will not only contain the constants $GF(p)$ but also some powers of β. We give a general form for the elements of $(DF(q,n))_d$, confirming what was proven in Theorem 2.1.14.

Theorem 2.1.16. *For $(DF(q,n)^*, \circ_\phi)$, if $b \in (DF(q,n))_d$ then*

$$b = \beta^{t(\frac{q^n-1}{q-1})} \quad \textit{for } t \in \{1, 2, \ldots, q-1\}$$

where β generates $(DF(q,n)^*, \circ_\phi)$.

Proof. Let $b \in (DF(q,n))_d$, then $b^{q^s} = b$ where $s \in \{1, 2, \ldots, n-1\}$. We want to show that b has the form $\beta^{t(\frac{q^n-1}{q-1})}$.
We will use mathematical induction to prove that for any $b \in (DF(q,n))_d$, where $b = \beta^{t(\frac{q^n-1}{q-1})}$, $t \in \{1, 2, \ldots, q-1\}$, that

$$\left(\beta^{t(\frac{q^n-1}{q-1})}\right)^{q^s} = \beta^{t(\frac{q^n-1}{q-1})} \pmod{q^n}$$

where $s \in \{1, 2, \ldots, n-1\}$.
Let us prove that our statement is true for $s = 1$: Using Fermat's Lemma,

$$\begin{aligned}
\left(\beta^{t(\frac{q^n-1}{q-1})}\right)^{q} &= \beta^{tq(\frac{q^n-1}{q-1})} \pmod{q^n} \\
&= \beta^{t(q^n+q^{n-1}+\ldots+q^2+q)} \pmod{q^n} \\
&= \beta^{tq^n}\beta^{t(q^{n-1}+\ldots+q^2+q+1-1)} \pmod{q^n} \\
&= (\beta^{q^n})^t(\beta^{t(q^{n-1}+\ldots+q+1)})\beta^{-t} \pmod{q^n} \\
&= \beta^t\beta^{t(\frac{q^n-1}{q-1})}\beta^{-t} \pmod{q^n} \\
&= \beta^{t(\frac{q^n-1}{q-1})} \pmod{q^n}
\end{aligned}$$

We assume that our statement is true for $s = k$:

$$\left(\beta^{t(\frac{q^n-1}{q-1})}\right)^{q^k} = \beta^{t(\frac{q^n-1}{q-1})}.$$

We now prove that our statement is true for $s = k + 1$:

$$\begin{aligned}\left(\beta^{t(\frac{q^n-1}{q-1})}\right)^{q^{k+1}} &= \beta^{tq^{k+1}(\frac{q^n-1}{q-1})} \pmod{q^n} \\ &= \beta^{tq^k(q^n+q^{n-1}+\ldots+q^2+q)} \pmod{q^n} \\ &= \beta^{tq^kq^n}\beta^{tq^k(q^{n-1}+\ldots+q^2+q+1-1)} \pmod{q^n} \\ &= (\beta^{q^n})^{q^k}t(\beta^{tq^k(q^{n-1}+\ldots+q+1)})\beta^{-tq^k} \pmod{q^n} \\ &= \beta^{tq^k}\beta^{tq^k(\frac{q^n-1}{q-1})}\beta^{-tq^k} \pmod{q^n} \\ &= \left(\beta^{t(\frac{q^n-1}{q-1})}\right)^{q^k} \pmod{q^n} \\ &= \beta^{t(\frac{q^n-1}{q-1})} \pmod{q^n}\end{aligned}$$

Hence, all $b \in (DF(q,n))_d$ will have the form $b = \beta^{t(\frac{q^n-1}{q-1})}$. □

We now give an example to illustrate the above corollary.

Example 2.1.17.
Consider the Dickson near-field $DF(9,2)$, where β is a generator of $GF(p^{ln}) = GF(3^4)$ and a root of the irreducible polynomial $f(x) = x^4+x+2$. Then the elements of $(DF(q,n))_d$ are listed below:

$$(DF(q,n))_d = \{\beta^{10}, \beta^{20}, \beta^{30}, \beta^{40} = 2, \beta^{50}, \beta^{60}, \beta^{70}, \beta^{80} = 1\}.$$

So the elements are of the form β^{10t} where $t \in \{1, 2, \ldots, 8\}$, so that

$$\begin{aligned}\left(\beta^{10t}\right)^9 &= \beta^{90t} \quad (mod\ 81) \\ &= \beta^{10t} \quad (mod\ 81).\end{aligned}$$

◊

Dickson used the form $H\beta^{\frac{q^k-1}{q-1}}$, for $k \in \{1, \ldots, n\}$, to represent the cosets of $(\mathrm{DF}(q,n)^*, \circ_\phi)$. In fact, for the class of finite Dickson near-fields where $n|(q-1)$, the following was proved in [11].

Lemma 2.1.18. *([11]) For a pair of Dickson numbers (q,n) such that $n|(q-1)$, the following is true for $u \in \{1, \ldots, n\}$:*

$$H\beta^{\frac{q^u-1}{q-1}} = H\beta^u.$$

This is not in general the case:

Example 2.1.19. *For the Dickson pair* $(5,8)$*, we have that* H *is generated by* β^8*, where* β *is the element that generates* $DF(5,8)^*$*. Then according to Dickson's form the cosets are listed as:*

$$\{H\beta, H\beta^6, H\beta^{31}, H\beta^{156}, H\beta^{781}, H\beta^{3906}, H\beta^{19531}, H\beta^{97656}\}.$$

Each of these cosets can be represented by a coset $H\beta^k$*, where* $k \in \{1,\dots,n\}$*. By inspection:*

$$\begin{aligned}
H\beta^{\frac{q^k-1}{q-1}} &= H\beta^k, \text{ where } k = \{1,4,5,8\}\\
H\beta^{\frac{q^2-1}{q-1}} &= H\beta^6\\
H\beta^{\frac{q^3-1}{q-1}} &= H\beta^7\\
H\beta^{\frac{q^6-1}{q-1}} &= H\beta^2\\
H\beta^{\frac{q^7-1}{q-1}} &= H\beta^3
\end{aligned}$$

The multiplication table for $DF(5,8)^*$ *is given by*

$\circ_\phi$	H	$H\beta$	$H\beta^6$	$H\beta^7$	$H\beta^4$	$H\beta^5$	$H\beta^2$	$H\beta^3$
H	H	$H\beta$	$H\beta^6$	$H\beta^7$	$H\beta^4$	$H\beta^5$	$H\beta^2$	$H\beta^3$
$H\beta$	$H\beta$	$H\beta^6$	$H\beta^7$	$H\beta^4$	$H\beta^5$	$H\beta^2$	$H\beta^3$	H
$H\beta^6$	$H\beta^6$	$H\beta^7$	$H\beta^4$	$H\beta^5$	$H\beta^2$	$H\beta^3$	H	$H\beta$
$H\beta^7$	$H\beta^7$	$H\beta^4$	$H\beta^5$	$H\beta^2$	$H\beta^3$	H	$H\beta$	$H\beta^6$
$H\beta^4$	$H\beta^4$	$H\beta^5$	$H\beta^2$	$H\beta^3$	H	$H\beta$	$H\beta^6$	$H\beta^7$
$H\beta^5$	$H\beta^5$	$H\beta^2$	$H\beta^3$	H	$H\beta$	$H\beta^6$	$H\beta^7$	$H\beta^4$
$H\beta^2$	$H\beta^2$	$H\beta^3$	H	$H\beta$	$H\beta^6$	$H\beta^7$	$H\beta^4$	$H\beta^5$
$H\beta^3$	$H\beta^3$	H	$H\beta$	$H\beta^6$	$H\beta^7$	$H\beta^4$	$H\beta^5$	$H\beta^2$

Note that $H\beta^3 \circ_\phi H\beta = H$*.* ◊

Thus for Dickson pairs (q,n) where $n|(q-1)$ we can easily predict in which coset a product ends up in, i.e. for $v,w \in \{0,1,\dots,n-1\}$:

$$H\beta^v \circ_\phi H\beta^w = H\beta^u \text{ if and only if } (v+w) \equiv u \bmod n.$$

2.2 Near-vector spaces

Next we turn our attention to what is known thus far about near-vector spaces. We begin with the definition of a near-vector space:

Definition 2.2.1. *([4]) A non-trivial near-vector space is a pair* (V,A) *which satisfies the following conditions:*

(a) $(V,+)$ *is a group and* A *is a set of endomorphisms of* V*;*
(b) A *contains the endomorphisms* 0*,* 1 *and* -1*, where* 1 *is the identity endomorphism and* -1 *the endomorphism defined by* $x(-1) = -x$ *for all* $x \in V$*;*
(c) $A^* = A\backslash\{0\}$ *is a subgroup of the group* $(Aut(V), \circ)$*;*
(d) If $x\alpha = x\beta$ *with* $x \in V$ *and* $\alpha, \beta \in A$*, then* $\alpha = \beta$ *or* $x = 0$*, i.e.* A *acts fixed point free on* V*;*
(e) The quasi-kernel $Q(V)$ *of* V*, generates* V *as a group, i.e. for all* $v \in V$*, there exists* $u_i \in Q(V)$*,* $\lambda_i \in A$ *for* $i \in \{1, \ldots, n\}$ *such that*

$$v = \sum_{i=1}^{n} u_i\lambda_i.$$

Here,

$$Q(V) = \{x \in V | \forall \alpha, \beta \in A,\ \exists \gamma \in A \text{ such that } x\alpha + x\beta = x\gamma\}.$$

We will write scalars on the right, as in [4] and Q for $Q(V)$ if it does not cause any confusion.

Remark 2.2.2.

- *The trivial near-vector space* $\{0\}$ *has to be dealt with as a separate case, since its automorphism group has no non-zero elements.*
- $(V,+)$ *is abelian since* $-1 \in A$ *and*

$$x + y = (-x)(-1) + (-y)(-1) = (-x - y)(-1) = (-(y + x))(-1) = y + x.$$

- *It is clear that every vector space is a near-vector space with* $Q(V) = V$*.*

André defined linear independence for subsets of Q in terms of a dependence relation (see [4]). He then stated that

Proposition 2.2.3. *([4]) A subset* M *of* Q *is independent if and only if for* $\lambda_i \in F$ *and distinct* $u_i \in M$*, where* $i = 1, 2, \ldots, n$*,* $\sum_{i=1}^{n} u_i\lambda_i = 0$*, implies that* $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$*.*

The *dimension* of the near-vector space, $\dim V$, is uniquely determined by the cardinality of an independent generating set for Q, called a *basis* of V, i.e. $\mathcal{B}$ is a basis for V if it is an independent subset of Q and for all $v \in Q(V)$ there exists a $u_i \in \mathcal{B}$, $\lambda_i \in A$ such that

$$v = \sum_{i=1}^{n} u_i\lambda_i.$$

We will make use of the following properties throughout the thesis:

Lemma 2.2.4. *([4]) The quasi-kernel $Q(V)$ of a near-vector space (V, A), has the following properties:*

(a) $0 \in Q(V)$;
(b) For $u \in Q(V)^*$, γ *is uniquely determined by* α *and* β *in the equation*

$$u\alpha + u\beta = u\gamma;$$

(c) If $u \in Q(V)$ *and* $\lambda \in A$, *then* $u\lambda \in Q$, *i.e.* $uA \subseteq Q(V)$;
(d) If $u \in Q(V)$ *and* $\lambda_i \in A$, *for* $i = 1, 2, \ldots, n$, *then*

$$\sum_{i=1}^{n} u\lambda_i = u\eta \in Q(V)$$

for some $\eta \in A$ *and for all integers* $n \geq 1$;
(e) If $u \in Q(V)^*$ *and* $\alpha, \beta \in A$, *then there exists a* $\gamma \in A$ *such that*

$$u\alpha - u\beta = u\gamma.$$

Remark 2.2.5.

- *Note by (c) above Q is closed under scalar multiplication. It is not in general closed under addition. This means that in axiom (e) of Definition 2.2.1 when we say Q generates V, we mean that for all $v \in V$, there exists a $u_i \in Q$ such that*

$$v = \sum_{i \in I} u_i \text{ for some index set } I.$$

- *A near-field F over itself is a near-vector space. This was shown in [15]: F is a near-field, so it contains the identity* 1. *For $\alpha, \beta \in F$, we have*

$$(1)(\alpha + \beta) = 1\alpha + 1\beta,$$

so $1 \in Q(F)$. Let $x \in F$, then $1x \in Q(F)$ since $Q(F)$ is closed under scalar multiplication. This implies that $F \subseteq Q(F)$ and since we have that $Q(F) \subseteq F$, we have that $Q(F) = F$. Hence, $Q(F)$ generates F.
- *The near-vector space (F, F) with F a near-field has $\{1\}$ as basis.*

For near-vector spaces, the notion of a subspace had to be defined in terms of the quasi-kernel.

Definition 2.2.6. *([16]) If (V, A) is a near-vector space and $\emptyset \neq W \subseteq V$ is such that W is the subgroup of $(V, +)$ generated additively by $XA = \{x\lambda \,|\, x \in X, \lambda \in A\}$, where X is an independent subset of $Q(V)$, then we say that (W, A) is a subspace of (V, A), or simply W is a subspace of V if A is clear from the context.*

Remark 2.2.7.

- *Since by Definition 2.2.6, X is a basis of W, the dimension of W is $|X|$. Any near-vector space is a subspace of itself since it is generated by a basis of its quasi-kernel.*
- *The trivial subspace, $\{0\}$, is the space generated by the empty subset of $Q(V)$.*

In [15] Howell proved that the quasi-kernel of the subspace, $Q(W)$, can be written in terms of W and the quasi-kernel of V.

Lemma 2.2.8. *([15]) If W is a subspace of V, then $Q(W) = W \cap Q(V)$.*

By Lemma 2.2.4(b), γ is uniquely determined by α and β. With this in mind, André defined a new operation on A as follows:

Definition 2.2.9. *([4]) Let (V, A) be a near-vector space, and let $u \in Q(V)^*$. Define the operation $+_u$ on A by*

$$u(\alpha +_u \beta) := u\alpha + u\beta$$

where $\alpha, \beta \in A$.

Remark 2.2.10.
If (V, A) is a vector space, then for all $u \in Q(V)^*$, $\alpha, \beta \in A$,

$$\alpha +_u \beta = \alpha + \beta.$$

Moreover, we have for (V, A) a near-vector space that for all $u \in Q(V)^*$,

$$\alpha +_u \beta = \gamma,$$

where $u\alpha + u\beta = u\gamma$.

Regularity is central in the study of near-vector spaces. André referred to the regular subspaces of a near-vector space as the building blocks of near-vector space theory. We begin by defining what a regular near-vector space is.

Definition 2.2.11. *([4]) A near-vector space (V, A) is regular if any two vectors of $Q(V)^*$ are compatible, i.e. if for any two vectors u and v of $Q(V)^*$ there exists a $\lambda \in A\backslash\{0\}$ such that $u + v\lambda \in Q(V)$.*

As we will see in the next corollary, the definition of a subspace of a near-vector space reduces to that of a vector space when A is a division ring.

Corollary 2.2.12. *([18]) Let (V, A) be a non-regular near-vector space and suppose $(A, +_v, \cdot)$ is a division ring for all non-zero $v \in Q(V)$. Then W is a subspace of V if and only if it is non-empty, closed under addition and scalar multiplication.*

It is clear that every vector space is regular, but this is not in general true for every near-vector space, as we will see. Before we discuss the regularity of near-vector spaces, we first examine the compatibility of elements in a near-vector space. Compatibility can be characterised in terms of the addition defined in Definition 2.2.9.

Lemma 2.2.13. *([4]) The elements $u, v \in Q(V)^*$ are compatible if and only if there exists a $\lambda \in A \setminus \{0\}$ such that $+_u = +_{v\lambda}$.*

We can define a relation on $Q(V)^*$ in terms of compatibility.

Definition 2.2.14. *([4]) Let (V, A) be a near-vector space. Then we define a relation $\sim$ on $Q(V)^*$ such that for $u, v \in Q(V)^*$, $u \sim v$ if and only if $u + v\lambda \in Q(V)$ for some $\lambda \in A^*$.*

Compatibility induces an equivalence relation on $Q(V)$.

Lemma 2.2.15. *([4]) Let (V, A) be a near-vector space. Then the relation $\sim$ is an equivalence relation on $Q(V)^*$.*

Thus compatibility partitions the non-zero elements of the quasi-kernel. The following result is useful for checking regularity.

Theorem 2.2.16. *([4]) A near-vector space V is regular if and only if there exists a basis which consists of mutually pairwise compatible vectors.*

It is clear that if $V = Q(V)$, V is regular, but the converse is not true in general. We will illustrate this with an example later in the thesis.

Lemma 2.2.17. *Suppose (V, A) is a near-vector space and W is a subspace of V. If V is regular, then W is regular.*

Proof. Suppose V is regular. Let $w_1, w_2 \in Q(W)^*$, then since by Lemma 2.2.8, $Q(W) = W \cap Q(V)$ we have that $w_1, w_2 \in Q(V)^*$. Thus there exists a $\lambda \in A^*$ such that $w_1 + w_2\lambda \in Q(V)^*$ since V is regular. Moreover, since W is a subspace of V, we also have that $w_1 + w_2\lambda \in W$ and thus $w_1 + w_2\lambda \in Q(W)$. Hence W is regular. □

Suppose we know that V is not a regular near-vector space, can it somehow be written in terms of regular subspaces? André answered this question in the next important theorem, called the Decomposition Theorem.

Theorem 2.2.18. *([4], The Decomposition Theorem) Every near-vector space (V, A) is the direct sum of regular near-vector spaces V_j $(j \in J)$ such that each $u \in Q(V)^*$ lies in precisely one direct summand V_j. The subspaces V_j are maximal regular near-vector spaces.*

We will not prove this theorem, but from the proof in [4], we will outline the procedure to decompose a near-vector space into its maximal regular subspaces:

- Partition $Q(V)^*$ into sets Q_j $(j \in J)$ of mutually pairwise compatible vectors.
- Let $\mathcal{B} \subseteq Q(V)^*$ be a basis of V and $B_j := \mathcal{B} \cap Q_j$.
- Let $V_j := \langle B_j \rangle$, be the subspace of V generated by B_j.
- Then each V_j will be a maximal regular subspace of V and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$.

By the Uniqueness Theorem ([4]) this decomposition is unique and is called the *canonical decomposition* of V. Thus it is evident that the study of near-vector spaces is largely reduced to the study of regular near-vector spaces.

In the following example we have a near-vector space which is not regular, and show how it is decomposed into two maximal regular near-vector spaces:

Example 2.2.19.
Let $V = A^4$ and $A = \mathbb{Z}_5$. Define scalar multiplication for all $(x_1, x_2, x_3, x_4) \in V$ and $\alpha \in A$ by

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3).$$

Then (V, A) is a near-vector space with basis given by

$$\mathcal{B} = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\}.$$

To verify this, we prove the axioms of a near-vector space:

(a) $(V, +)$ is a group.
This follows from elementary group theory.

(b) A is a set of endomorphisms of $(V, +)$ such that $0, 1, -1 \in A$.
For $\alpha \in A$ and $(x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \in V$ we have

$$\begin{aligned}
[(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4)]\alpha &= (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)\alpha \\
&= ((x_1 + y_1)\alpha, (x_2 + y_2)\alpha^3, (x_3 + y_3)\alpha, (x_4 + y_4)\alpha^3) \\
&= (x_1\alpha + y_1\alpha, x_2\alpha^3 + y_2\alpha^3, x_3\alpha + y_3\alpha, x_4\alpha^3 + y_4\alpha^3) \\
&= (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3) + (y_1\alpha, y_2\alpha^3, y_3\alpha, y_4\alpha^3) \\
&= (x_1, x_2, x_3, x_4)\alpha + (y_1, y_2, y_3, y_4)\alpha
\end{aligned}$$

Hence, α acts as an endomorphism on V. Furthermore,

(i) $(x_1, x_2, x_3, x_4)0 = (x_1 0, x_2 0^3, x_3 0, x_4 0^3) = (0, 0, 0, 0)$;
(ii) $(x_1, x_2, x_3, x_4)1 = (x_1 1, x_2 1^3, x_3 1, x_4 1^3) = (x_1, x_2, x_3, x_4)$;
(iii)

$$\begin{aligned}(x_1, x_2, x_3, x_4)(-1) &= (x_1, x_2, x_3, x_4)4 \\ &= (x_1 4, x_2 4^3, x_3 4, x_4 4^3) \\ &= (x_1 4, x_2 4, x_3 4, x_4 4) \\ &= (x_1(-1), x_2(-1), x_3(-1), x_4(-1)) \\ &= (-x_1, -x_2, -x_3, -x_4)\end{aligned}$$

(c) $(A^8, \cdot)$ *is a subgroup of* $(Aut(V), \circ)$.
Let $\alpha \in A^*$ *where* $A^* = \{1, 2, 3, 4\}$, *and suppose* $(x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \in V$.

(i) A *is a set of endomorphisms on* V, *so* α *is an endomorphism.*

(ii) α *is injective;*
Suppose $(x_1, x_2, x_3, x_4)\alpha = (y_1, y_2, y_3, y_4)\alpha$, *then*

$$\begin{aligned}(x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3) &= (y_1\alpha, y_2\alpha^3, y_3\alpha, y_4\alpha^3) \\ (x_1\alpha - y_1\alpha, x_2\alpha^3 - y_2\alpha^3, x_3\alpha - y_3\alpha, x_4\alpha^3 - y_4\alpha^3) &= 0\end{aligned}$$

This implies that $x_1\alpha - y_1\alpha = 0$, $x_2\alpha^3 - y_2\alpha^3 = 0$, $x_3\alpha - y_3\alpha = 0$ *and* $x_4\alpha - y_4\alpha^3 = 0$. *Since* $\alpha \neq 0$, *we have that* $x_i = y_i$ *for* $i \in \{1, 2, 3, 4\}$. *Hence,* $(x_1, x_2, x_3, x_4) = (y_1, y_2, y_3, y_4)$.

(iii) α *is surjective;*
Suppose $(y_1, y_2, y_3, y_4) \in V$ *and* $\alpha \in A^*$. *We need to prove that there exists an element* $(x_1, x_2, x_3, x_4) \in V$ *such that* $(x_1, x_2, x_3, x_4)\alpha = (y_1, y_2, y_3, y_4)$. *But we can take* $(x_1, x_2, x_3, x_4) = (y_1\alpha^{-1}, y_2\alpha^{-3}, y_3\alpha^{-1}, y_4\alpha^{-3}) \in V$ *so that* $(y_1\alpha^{-1}, y_2\alpha^{-3}, y_3\alpha^{-1}, y_4\alpha^{-3})\alpha = (y_1, y_2, y_3, y_4)$. *Hence,* α *is surjective.*

Hence, $(A^*, \cdot)$ *is a subset of the automorphism group of* V *under composition. We need to show that* $(A^*, \cdot)$ *is a subgroup of* $(Aut(V), \circ)$.
Suppose $\alpha, \beta \in A^*$, *then* $\beta^{-1} \in A^*$ *since* A *is a field. We first show that* $\alpha\beta^{-1} \in A^*$. *We have*

$$\begin{aligned}(x_1, x_2, x_3, x_4)(\alpha\beta^{-1}) &= (x_1\alpha\beta^{-1}, x_2(\alpha\beta^{-1})^3, x_3\alpha\beta^{-1}, x_4(\alpha\beta^{-1})^3) \\ &= (x_1\alpha\beta^{-1}, x_2\alpha^3\beta^{-3}, x_3\alpha\beta^{-1}, x_4\alpha^3\beta^{-3}) \\ &\in V,\end{aligned}$$

which implies that $\alpha\beta^{-1} \in A^*$. *Finally, we show that* $\alpha\beta^{-1}$ *is an endomorphism.*

Let $(x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \in V$, *then*

$$\begin{aligned}[(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4)]\alpha\beta^{-1} &= (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)\alpha\beta^{-1} \\ &= ((x_1 + y_1)\alpha\beta^{-1}, (x_2 + y_2)(\alpha\beta^{-1})^3, (x_3 + y_3)\alpha\beta^{-1}, \\ &\quad (x_4 + y_4)(\alpha\beta^{-1})^3) \\ &= (x_1\alpha\beta^{-1} + y_1\alpha\beta^{-1}, x_2(\alpha\beta^{-1})^3 + y_2(\alpha\beta^{-1})^3, \\ &\quad x_3\alpha\beta^{-1} + y_3\alpha\beta^{-1}, x_4(\alpha\beta^{-1})^3 + y_4(\alpha\beta^{-1})^3) \\ &= (x_1\alpha\beta^{-1}, x_2(\alpha\beta^{-1})^3, x_3\alpha\beta^{-1}, x_4(\alpha\beta^{-1})^3) + \\ &\quad (y_1\alpha\beta^{-1}, y_2(\alpha\beta^{-1})^3, y_3\alpha\beta^{-1}, y_4(\alpha\beta^{-1})^3) \\ &= (x_1, x_2, x_3, x_4)\alpha\beta^{-1} + (y_1, y_2, y_3, y_4)\alpha\beta^{-1}.\end{aligned}$$

Therefore, $(A^*, \cdot)$ *is a subgroup of* $(Aut(V), \circ)$.

(d) A *acts fixed-point-free on* V.
Suppose $(x_1, x_2, x_3, x_4) \in V$ *and* $\alpha, \beta \in A$. *Then*

$$\begin{aligned}(x_1, x_2, x_3, x_4)\alpha &= (x_1, x_2, x_3, x_4)\beta, \text{ implies that,} \\ (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3) &= (x_1\beta, x_2\beta^3, x_3\beta, x_4\beta^3),\end{aligned}$$

which implies that $x_1\alpha = x_1\beta$, $x_2\alpha^3 = x_2\beta^3$, $x_3\alpha = x_3\beta$ *and* $x_4\alpha^3 = x_4\beta^3$. *If* $\alpha \neq \beta$, *then* $\alpha^3 \neq \beta^3$ *and* $x_1 = x_2 = x_3 = x_4 = 0$, *that is,* $(x_1, x_2, x_3, x_4) = (0, 0, 0, 0)$.

(e) The quasi-kernel $Q(V)$ *of* V *contains all elements* $v \in V$ *such that for all* $\alpha, \beta \in A$ *there exists a* $\gamma \in A$ *such that* $v\alpha + v\beta = v\gamma$.

(i) Let $(a, 0, c, 0) \in V$, *then for* $\alpha, \beta \in A$,

$$\begin{aligned}(a, 0, c, 0)\alpha + (a, 0, c, 0)\beta &= (a\alpha, 0, c\alpha, 0) + (a\beta, 0, c\beta, 0) \\ &= (a\alpha + a\beta, 0, c\alpha + c\beta, 0) \\ &= (a(\alpha + \beta), 0, c(\alpha + \beta), 0) \\ &= (a, 0, c, 0)(\alpha + \beta) \\ &= (a, 0, c, 0)\gamma.\end{aligned}$$

Therefore, $(a, 0, c, 0) \in Q(V)$ *for each* $a, c \in A$.

(ii) Let $(0, b, 0, d) \in V$, *then for* $\alpha, \beta \in A$,

$$\begin{aligned}(0, b, 0, d)\alpha + (0, b, 0, d)\beta &= (0, b\alpha^3, 0, d\alpha^3) + (0, b\beta^3, 0, d\beta^3) \\ &= (0, b\alpha^3 + b\beta^3, 0, d\alpha^3 + d\beta^3) \\ &= (0, b(\alpha^3 + \beta^3), 0, d(\alpha^3 + \beta^3)) \\ &= (0, b, 0, d)(\alpha^3 + \beta^3)^{1/3} \\ &= (0, b, 0, d)\gamma,\end{aligned}$$

where $\gamma = (\alpha^3 + \beta^3)^{1/3} \in A$ *by a well-known result (See [1], for example). Therefore,* $(0, b, 0, d) \in Q(V)$ *for each* $b, d \in A$. *A quick check shows that these are the only elements belonging to* $Q(V)$.

The quasi-kernel of V is given by

$$Q(V) = \{(a, 0, c, 0)|a, c \in A\} \cup \{(0, b, 0, d)|b, d \in A\}.$$

V is not regular since, for example, for any $a, d \in A$ and $\alpha \neq 0$, $(a, 0, 0, 0) + (0, 0, 0, d)\alpha = (a, 0, 0, d\alpha^3) \notin Q(V)$.

We can therefore decompose V into maximal regular near-vector spaces as follows: We partition $Q(V)^* = Q(V) \setminus \{(0, 0, 0, 0)\}$ into pairwise mutually disjoint sets, say Q_1 and Q_2, where

$$Q_1 = \{(a, 0, c, 0)|a, c \in A\} \setminus \{(0, 0, 0, 0)\},$$

and

$$Q_2 = \{(0, b, 0, d)|b, d \in A\} \setminus \{(0, 0, 0, 0)\}.$$

Then

$$B_1 = \mathcal{B} \cap Q_1 = \{(1, 0, 0, 0), (0, 0, 1, 0)\},$$

and

$$B_2 = \mathcal{B} \cap Q_2 = \{(0, 1, 0, 0), (0, 0, 0, 1)\}.$$

We then define V_1 and V_2 to be the near-vector spaces generated by B_1 and B_2, respectively:

$$V_1 := \langle B_1 \rangle = \{(1, 0, 0, 0)a + (0, 0, 1, 0)c|a, c \in A\} = \{(a, 0, c, 0)|a, c \in A\},$$

and

$$V_2 := \langle B_2 \rangle = \{(0, 1, 0, 0)b + (0, 0, 0, 1)d|b, d \in A\} = \{(0, b, 0, d)|b, d \in A\}.$$

By the Decomposition Theorem, $V = V_1 \oplus V_2$, where V_1 and V_2 are maximal regular near-vector spaces. It is interesting to note that V_1 is in fact a vector space over A. $\Diamond$

Next, we define what a linear mapping is:

Definition 2.2.20. *([16]) Let (V_1, A) and (V_2, A) be near-vector spaces over A. A function $T : V_1 \to V_2$ is a linear mapping from V_1 to V_2 if*

$$T(v_1 + v_2) = T(v_1) + T(v_2) \text{ for all } v_1, v_2 \in V_1$$

and

$$T(v\alpha) = T(v)\alpha \text{ for all } v \in V_1 \text{ and } \alpha \in A.$$

In [21] linear mappings of near-vector spaces were investigated. In particular, the linear mappings of near-vector spaces constructed from $\mathbb{R}$ and finite fields were studied. We will give an example of a linear mapping of a near-vector space over a finite field.

Example 2.2.21.
Let $V = A^4$ be the near-vector space, with $A = GF(3^2)$ and scalar multiplication defined for all $(x_1, x_2, x_3, x_4) \in V$ and $\alpha \in A$ by

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3).$$

Then the set of linear mappings of V over A, $L_A(V)$, is given by

$$L_A(V) = \begin{pmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{pmatrix}.$$

$\Diamond$

Linear mappings preserve regularity.

Lemma 2.2.22. *([16])Let T be a linear mapping from (V, A) into (W, A). If V_j is a regular subspace of V, then $T(V_j)$ is a regular subspace of W.*

Linear mappings map the quasi-kernel of the one space to the quasi-kernel of the other space.

Proposition 2.2.23. *([12]) Let (V_1, A) and (V_2, A) be near-vector spaces over A and $T : V_1 \to V_2$ a linear mapping. Then $T(Q(V_1)) \subseteq Q(V_2)$.*

Next, we define when two near-vector spaces are isomorphic:

Definition 2.2.24. *([19]) We say that two near-vector spaces (V_1, A_1) and (V_2, A_2) are isomorphic (written $(V_1, A_1) \cong (V_2, A_2)$) if there are group isomorphisms $\theta : (V_1, +) \to (V_2, +)$ and $\eta : (A_1^*, \cdot) \to (A_2^*, \cdot)$ such that $\theta(x\alpha) = \theta(x)\eta(\alpha)$ for all $x \in V_1$ and $\alpha \in A_1^*$. We will denote an isomorphism as a pair (θ, η).*

When two near-vector spaces are isomorphic, we can say more about their quasi-kernels.

Theorem 2.2.25. *([17]) If the near-vector spaces (V_1, A_1) and (V_2, A_2) are isomorphic, say (θ, η) is the isomorphism, then $\theta(Q(V_1)) = Q(V_2)$.*

The next example shows that it is possible for two near-vector spaces to be isomorphic, even though one may be a vector space.

Example 2.2.26.
Let both $(V_1, +)$ *and* $(V_2, +)$ *be given by* $((\mathbb{Z}_5)^2, +)$. *Suppose* (V_1, A_1) *is the near-vector space where we define the scalar multiplication as normal multiplication, with* $A_1 = \mathbb{Z}_5$. *For* (V_2, A_2) *we define for all* $(v_1, v_2) \in V_2$, $\alpha \in A_2 = \mathbb{Z}_5$, *the scalar multiplication* $(v_1, v_2)\alpha = (v_1\alpha^3, v_2\alpha^3)$. *Then by taking the pair* (θ, η) *where:*

$$\begin{aligned} \theta : (V_1, +) &\to (V_2, +) \\ x &\mapsto x \end{aligned}$$

and

$$\begin{aligned} \eta : (A_1^*, \cdot) &\to (A_2^*, \cdot) \\ \alpha &\mapsto \alpha^{1/3}, \end{aligned}$$

we see that $(V_1, A_1) \cong (V_2, A_2)$ *as near-vector spaces. Note that* (V_1, A_1) *is a vector space, while* (V_2, A_2) *is not.* ◊

We will need the following proposition later:

Proposition 2.2.27. *([12]) If the near-vector spaces* (V_1, A_1) *and* (V_2, A_2) *are isomorphic, then* $v \in Q(V_1)$ *implies that* $\theta(v) \in Q(V_2)$, *where* (θ, η) *is the isomorphism from* V_1 *to* V_2.

Later in this thesis, we will study the fibrations of near-vector spaces. We introduce some definitions we will need.

Definition 2.2.28. *([17]) A fibered group* $(V, +, \mathcal{F})$, *with identity* 0 *is a group* $(V, +)$ *with a fibration, i.e. a set* $\mathcal{F}$ *of subgroups of* V *such that any element of* V *different from* 0 *belongs to exactly one such subgroup. The subgroups are called the fibers of* $\mathcal{F}$.

We now define a new relation which we will see is related to the fibers.

Definition 2.2.29. *([17]) Let* (V, A) *be a near-vector space. We define a relation* $\asymp$ *on* V *such that for* $u, v \in V$, $u \asymp v$ *if and only if* $v = u\lambda$ *for some* $\lambda \in A^*$.

It is not difficult to verify that the relation $\asymp$ defined above is an equivalence relation on V. The nonzero equivalence classes of $\asymp$, called the pseudo-projective space of V is denoted by $P(V)$.

Definition 2.2.30. *([17]) Let* (V, A) *be a near-vector space. Then the pseudo-projective space* $P(V)$ *induced by* V *is the set of equivalence classes of* V^* *under the equivalence relation defined by* $\asymp$.

From [17] we have,

Lemma 2.2.31. *([17]) Let (V, A) be a near-vector space with $Q(V) = V$. Then the non-zero equivalence classes of the relation $\asymp$ are exactly the fibers bA^* for $b \in Q(V)^*$.*

A particular class of near-vector spaces has a natural fibered group associated with them.

Theorem 2.2.32. *([17]) Let (V, A) be a near-vector space. Then $(V, +, \mathcal{F})$ is a fibered group where $\mathcal{F} = \{bA \mid b \in Q(V)^*\}$ if and only if $Q(V) = V$.*

We note that the fibers in the theorem above are just the orbits of the action of A on V^*. Thus we are investigating when the orbits of the action of A on V^* will be subgroups of $(V, +)$.

2.2.1 Finite-dimensional near-vector spaces

In [30], van der Walt proved that finite-dimensional near-vector spaces can be constructed by taking copies of a finite number of near-fields that are multiplicatively isomorphic.

Theorem 2.2.33. *([30], van der Walt's theorem) Let $(G, +)$ be a group and let $A = D \cup \{0\}$, where D is a fixed point free group of automorphisms of G. Then (G, A) is a finite-dimensional near-vector space if and only if there exist a finite number of near-fields $F_1, \ldots, F_m$, semigroup isomorphisms $\psi_i : (A, \circ) \to (F_i, \cdot)$, and an additive group isomorphism $\Phi : G \to F_1 \oplus \ldots \oplus F_m$ such that if $\Phi(g) = (x_1, \ldots, x_m)$, then $\Phi(g\alpha) = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha))$ for all $g \in G$, $\alpha \in A$.*

According to this theorem, we can take F to be a near-field. Put $V = F^m$, $m \in \mathbb{Z}^+$ and let $\psi_i : (F, \cdot) \to (F, \cdot)$ for $1 \leq i \in \{1, \ldots, m\}$, be semigroup automorphisms. We define the scalar multiplication for all $\alpha \in F$ and $(x_i) \in V$ by

$$(x_1, \ldots, x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)). \tag{2.1}$$

We will denote a specific instance of this construction by (V, F).

In [16] near-vector spaces over near-fields were investigated. The near-vector space (V, F) where $V = F^m$, F is a near-field, $m \in \mathbb{Z}^+$ and all the ψ_i's are the identity for $i \in \{1, 2, \ldots, m\}$, is the near-vector space closest to traditional vector spaces. Thus the scalar multiplication is defined for all $\alpha \in F$, $(x_i) \in V$, $i \in \{1, \ldots, m\}$ by

$$(x_1, x_2, \ldots, x_m)\alpha = (x_1\alpha, x_2\alpha, \ldots, x_m\alpha).$$

For this near-vector space it was shown that it is regular. The following theorem from [22] describes the quasi-kernel. Let $I := \{1, 2, \ldots, m\}$.

Theorem 2.2.34. *([22]) Let F be a near-field and $V = F^m$, $n \in \mathbb{N}$ be a near-vector space with the scalar multiplication defined for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$ by*

$$(x_1, \ldots, x_m)\alpha = (x_1\psi(\alpha), \ldots, x_m\psi(\alpha)),$$

where ψ is an automorphism of $(F, \cdot)$. Then

$$Q(V) = \{(d_i)\lambda | \lambda \in F, d_i \in F_d \text{ for all } i \in I\}.$$

We mentioned earlier that $Q(V) = V$ implies that V is regular but the converse is not true. We illustrate this in the next example.

Example 2.2.35.
Let us consider the Dickson near-field of Example 2.1.13 again, where $F = DF(3, 2)$. Put $V = F^3$ and define for all $(x_1, x_2, x_3) \in V$ and $\alpha \in F$,

$$(x_1, x_2, x_3)\alpha = (x_1\alpha, x_2\alpha, x_3\alpha).$$

Then

$$Q(V) = \{(d_1, d_2, d_3)\lambda | \lambda \in F,\ d_i \in F_d \text{ for all } i \in I\},$$

where $F_d = \mathbb{Z}_3$. Note that $Q(V) \neq V$, since, for example, $(1+\beta, 2+\beta, \beta) \in V$ but it is not in $Q(V)$. If this was in $Q(V)$, then $(1 + \beta, 2 + \beta, \beta) = (d_1, d_2, d_3)\alpha$ for some $\alpha \in F$, but a quick check shows this is impossible. However, V is regular by Theorem 2.2.16, since $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ is a basis for V, consisting of mutually compatible vectors. $\Diamond$

The case where F is taken to be a finite field in the construction of (V, F) will be important in this thesis. Let $\mathrm{GF}(p^r)$ be the finite field of p^r elements, where p is a prime and r a positive integer. In order to use van der Walt's construction theorem, we first need the multiplicative automorphisms of $GF(p^r)^*$.

Proposition 2.2.36. *([7]) The mapping $\psi : GF(p^r)^* \to GF(p^r)^*$ is an automorphism of the group $(GF(p^r)^*, \cdot)$ if and only if there exists $s \in \mathbb{Z}$, with $1 \leq s \leq p^r - 1$ and $gcd(s, p^r - 1) = 1$, such that $\psi(x) = x^s$ for all $x \in GF(p^r)^*$.*

Thus every ψ_i, $i \in \{1, 2, \ldots, m\}$, defined in equation (2.1) is a s-th power function for some s, with $1 \leq s \leq p^r - 1$ and $\gcd(s, p^r - 1) = 1$.

In [19] suitable sequences were introduced as a tool to construct and count near-vector spaces.

Definition 2.2.37. *([19]) A finite sequence of k integers $s_1, s_2, \ldots, s_k$ is called suitable with respect to $F = GF(p^r)$ if*

(a) $1 \leq s_i \leq p^r - 1$ *and* $gcd(s_i, p^r - 1) = 1$ *for all* $i = 1, \ldots, k$;

(b) no s_i *can be replaced by a smaller* s_i' *that also satisfies (a) and such that* $s_i \equiv s_i' p^l$ *(mod* $p^r - 1$*) for some* $l \in \{0, 1, \ldots, r-1\}$.

For a given suitable sequence $(S) = (s_1, s_2, \ldots, s_k)$, we use $S := \{s_1, \ldots, s_N\}$ to denote the order set of all distinct elements in (S). To obtain a suitable sequence, list all cosets determined by the subgroup $\langle p \rangle$ of the multiplicative group $U(p^r - 1) = \{t \in \mathbb{Z} | 1 \leq t \leq p^r - 1 \text{ and } \gcd(t, p^r - 1) = 1\}$. Select any k members from the list - repetition may occur. Write them down in non-decreasing order.

In the following example, we illustrate the above sequences for $GF(3^3)$.

Example 2.2.38.
We look at 4-dimensional near-vector spaces determined by $F = GF(3^3)$. *Let* $V = F^4$, *then the set of cosets determined by* $\langle 3 \rangle$ *in the group* $U(3^3 - 1)$ *is*

$$\{\{1, 3, 9\},\ \{5, 15, 19\},\ \{7, 11, 21\},\ \{17, 23, 25\}\}.$$

All possible suitable sequences are determined by $\{1, 5, 7, 17\}$. *If we take the sequence* $(1, 1, 5, 17)$, *say, then it will define a near-vector space* (V, F), *with scalar multiplication defined for all* $(x_1, x_2, x_3, x_4) \in V$ *and all* $\alpha \in F$, *by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha, x_3\alpha^5, x_4\alpha^{17}).$$

$\Diamond$

The following theorem was proved in [27] and shows when near-vector spaces with suitable sequences, where the first entry is 1, are isomorphic.

Theorem 2.2.39. *([27]) Let* (F^m, F_1) *and* (F^m, F_2) *be near-vector spaces, where* F *is a finite field and* F_1 *and* F_2 *are determined by suitable sequences* (S_1) *and* (S_2), *respectively. Then* $(F^m, F_1) \cong (F^m, F_2)$ *if and only if there is* $s \in S_1$ *such that* $S_1 = sS_2$ *and the occurrences of* $ss_j' \in (S_1)$ *and* $s_j' \in (S_2)$ *are the same for each* $j = 1, \ldots, N$, *where* $N = |S_1| = |S_2|$.

Suppose $S_2 = \{1, q_2, \ldots, q_N\}$, then sS_2 is defined as $sS_2 = \{s, sq_2, \ldots, sq_N\}$, where the product $sq_i \equiv s_i \bmod q^n - 1$, for $i \in \{2, \ldots, N\}$, and s_i is the smallest element of the coset that contains the remainder of $\dfrac{sq_i}{q^n - 1}$.

Example 2.2.40. *([27])*
Consider the near-vector spaces, (V, F_1) *and* (V, F_2), *where* $V = F^4$, $F = GF(3^3)$ *and* F_1^* *and* F_2^* *are determined by the suitable sequences* $(S_1) = (1, 1, 5, 5)$ *and* $(S_2) = (1, 1, 7, 7)$,

respectively. In this case, by taking $s = 5$*, we see that the near-vector spaces* (V, F_1) *and* (V, F_2) *with scalar multiplication defined for all* $(x_1, x_2, x_3, x_4) \in V$ *and* $\alpha \in F_1$, $\alpha \in F_2$ *by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha, x_3\alpha^5, x_4\alpha^5)$$

and

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha, x_3\alpha^7, x_4\alpha^7),$$

respectively, are isomorphic, by Theorem 2.2.39. ◊

The following result in [7] by S.P. Sanon shows how we can construct regular near-vector spaces from copies of finite fields.

Lemma 2.2.41. *([7]) Let* $V = F^m$ *be a near-vector space, where* $F = GF(p^r)$*, with scalar multiplication defined for all* $(x_1, x_2, x_3, x_4) \in V$ *and* $\alpha \in F$ *by*

$$(x_1, \ldots, x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the ψ_i*'s are automorphisms of* $(F, \cdot)$*. Then* V *is regular if and only if for all* $i, j \in I$ *and* $\alpha \in GF(p^r)$*,* $\psi_i(\alpha) = \psi_j(\alpha^{p^l})$*, for some* $l \in \{0, \ldots, r-1\}$*.*

Remark 2.2.42.
Referring back to Example 2.2.38, since our suitable sequence elements were chosen from different cosets the near-vector spaces we constructed is non-regular. We will return to suitable sequences in the last chapter. Note that not all near-vector spaces have to be constructed using a suitable sequence, but every near-vector space of the form (V, F) *will be isomorphic to a near-vector space constructed using a suitable sequence.*

We illustrate the above lemma with the following example.

Example 2.2.43.
Let $V = F^4$ *where* $F = GF(3^3)$*. Define scalar multiplication for all* $(x_1, x_2, x_3, x_4) \in V$ *and* $\alpha \in F$ *by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^9).$$

According to Lemma 2.2.41, V *is regular since*

$$\begin{aligned}\psi_2(\alpha^3) &= (\alpha^3)^3\\ &= \alpha^9\\ &= \psi_4(\alpha),\end{aligned}$$

and

$$\begin{aligned}\psi_1(\alpha^9) &= \alpha^9\\ &= \psi_4(\alpha).\end{aligned}$$

◊

We now introduce two types of block constructions we will study. For the first, consider the near-vector space (V, F) where $F = GF(p^r)$, p a prime, $r \in \mathbb{Z}^+$. We use Lemma 2.2.41 to partition the set $I = \{1, \ldots, m\}$ as follows. Let $A_i = \{j \in I | \psi_i(\alpha) = \psi_j(\alpha^{p^l})$ for $\alpha \in F$ and some $l \in \{0, 1, \ldots, r-1\}\}$. The A_i, for $i \in K := \{1, \ldots, k\}$ are called the blocks of the construction.

In [7] the following result was proved.

Lemma 2.2.44. *([7]) For the near-vector space defined above we have:*

1. $Q(V) = \bigcup_{t=1}^{k} V_t$ *where,*
   $V_t = \{(0, 0, \ldots, a_1, 0, a_2, 0, \ldots, a_s, 0) | a_i \in F, a_i$ *is in position* l *with* $l \in A_t\}$, *for* $t \in K$.
2. *Each of the* V_t *is a regular subspace of* V.
3. $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ *is the canonical decomposition of* V.

Example 2.2.45.
Referring back to Example 2.2.19, with $V = (\mathbb{Z}_5)^4$, $F = \mathbb{Z}_5$ *and scalar multiplication defined for all* $(x_1, x_2, x_3, x_4) \in V$ *and* $\alpha \in F$ *by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3).$$

Then

$$Q(V) = V_1 \cup V_2,$$

where $V_1 = \{(a, 0, c, 0) \,|\, a, c \in F\}$ *and* $V_2 = \{(0, b, 0, d) \,|\, b, d \in F\}$. ◊

The following result shows that for this particular construction regularity is equivalent to the quasi-kernel being the whole of V.

Theorem 2.2.46. *([17]) Let* $F = GF(p^r)$ *and* $V = F^m$ *be a near-vector space with scalar multiplication defined for all* $(x_1, x_2, x_3, x_4) \in V$ *and* $\alpha \in F$ *by*

$$(x_1, \ldots, x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the $\psi_i's$ *are automorphisms of* $(F, \cdot)$. *Then the following are equivalent:*

1. $Q(V) = V$;
2. V *is regular;*
3. *for all* $i, j \in \{1, \ldots, m\}$ *and* $\alpha \in GF(p^r)$, $\psi_i(\alpha) = \psi_j(\alpha^{p^l})$, *for some* $l \in \{0, 1, \ldots, r-1\}$.

The next result generalises the previous theorem for the case where A is a division ring.

Theorem 2.2.47. *([18]) Let (V, A) be a near-vector space. The following assumptions are equivalent:*

1. *For any $v \in Q(V)^*$, V is a vector space over the near-field $(A, +_v, \cdot)$;*
2. *There is a $v \in Q(V)^*$, such that V is a vector space over the near-field $(A, +_v, \cdot)$;*

1.' *For any $v \in Q(V)^*$, V is a vector space over the near-field $(A, +_v, \cdot)$ and $(A, +_v, \cdot)$ is a division ring;*

2.' *There is a $v \in Q(V)^*$, such that V is a vector space over the near-field $(A, +_v, \cdot)$ and $(A, +_v, \cdot)$ is a division ring;*

3. *$Q(V) = V$ and $(A, +_v, \cdot)$ is a division ring, for all $v \in Q(V)^*$;*
4. *$+_v = +_w$ for all $v, w \in Q(V)^*$;*
5. *$R_w(V) = V$ for all $w \in Q(V)^*$;*
6. *V is regular and for any $v \in V$, $+_v = +_{v\theta}$ for all $v \in Q(V)^*$ and $\theta \in A$;*
7. *V is regular and for any $v \in Q(V)^*$, $(A, +_v, \cdot)$ is a division ring.*

In closing we give an example of a block construction using a finite Dickson near-field. Let $V = F^m$, where F is a finite Dickson near-field and $n \in \mathbb{N}$ and let

$$A_1 \cup A_2 \cup \cdots \cup A_k$$

be a partition of $\{1, \ldots, m\}$ where the A_i are mutually disjoint and nonempty. Suppose that all automorphisms ψ_i are equal for all $i \in A_t$ and each $t \in \{1, \ldots, k\}$. We call the A_i's blocks and say that (V, F) is constructed using these blocks.

Example 2.2.48.
Referring back to Example 2.1.13, where the Dickson near-field is constructed from the Dickson pair $(3, 2)$ with β being the root of $f(x) = x^2 + x + 2$. Let $V = F^3$ and $F = DF(3, 2)$. Define $\theta : DF(3, 2) \to DF(3, 2)$ by

$$\begin{aligned}
\theta : \ & 0 && \mapsto 0 \\
& 1 && \mapsto 1 \\
& 2 && \mapsto 2 \\
& \beta && \mapsto 2\beta \\
& 2\beta && \mapsto \beta \\
& 1 + \beta && \mapsto 2 + 2\beta \\
& 2 + 2\beta && \mapsto 1 + \beta \\
& 2 + \beta && \mapsto 2 + \beta \\
& 1 + 2\beta && \mapsto 1 + 2\beta.
\end{aligned}$$

In other words, θ takes each element in $H\beta$ to its additive (and in the case of this Dickson near-field, multiplicative) inverse, and each element in H to itself. It is also an automorphism with respect to $\circ_\phi$. Define for all $(x_1, x_2, x_3) \in V$ and $\alpha \in F$,

$$(x_1, x_2, x_3)\alpha := (x_1\alpha, x_2\alpha, x_3\theta(\alpha)).$$

We note we have the partition $A_1 = \{1, 2\}$ *and* $A_2 = \{3\}$. *Then* $Q(V) = V_1' \cup V_2'$, *with* $V_1' = \{(d_1, 0, 0)\lambda_1 + (0, d_2, 0)\lambda_2 | \lambda_1, \lambda_2 \in F \text{ and } d_1, d_2 \in F_d\}$, $V_2' = \{(0, 0, 1)\lambda | \lambda \in F\}$ *and* $\mathcal{B} = \{(0, 0, 1), (1, 0, 0), (0, 1, 0)\}$ *is a basis for* V. *For example, consider the elements* $(1, 2, 0)$ *and* $(0, 0, 2)$ *of* $Q(V)^*$. *If* V *were regular, then we would be able to find a* $\lambda \in F^*$ *such that* $(1, 2, 0) + (0, 0, 1)\lambda \in Q(V)$. *However*

$$\begin{aligned}(1, 2, 0) + (0, 0, 1)\lambda &= (1, 2, \theta(\lambda)) \\ &\notin Q(V).\end{aligned}$$

Therefore, V *is not regular. The canonical decomposition of* V *is given by* $V = V_1 \oplus V_2$, *with* $V_1 = \{(a, b, 0) | a, b \in F\}$ *and* $V_2 = \{(0, 0, c) | c \in F\}$. ◊

In Theorem 2.2.32 it was shown that for a near-vector space (V, A), the elements of the fibration are multiples of the non-zero elements of the quasi-kernel if and only if $Q(V) = V$. We would like to say something more for the fibrations of near-vector spaces of the form (V, F).

Lemma 2.2.49. *([23]) Let* (V, F) *be the near-vector space, where* F *is a proper near-field and* $m > 1$. *Then* $Q(V) \neq V$.

For F a proper near-field, we have only one case where a near-vector space of the form (V, F) has that $Q(V) = V$.

Lemma 2.2.50. *([23]) The near-vector space* (F, F), *where* F *is a proper near-field and the multiplication of* F *defines the scalar multiplication has* $Q(F) = F$.

We also have the following result:

Theorem 2.2.51. *([23]) The near-vector space* (V, F) *with* $m > 1$ *has* $Q(V) = V$ *if and only if* F *is a field and* (V, F) *is regular.*

Therefore, we have two cases where (V, F) has $Q(V) = V$. The first is when (F, F) is a near-vector space under the near-field multiplication, and the second is when we construct a regular near-vector space by taking copies of a finite field F. In the next result, we prove that if $A = F$ is a finite Dickson near-field, then the elements of the fibration are determined by the non-zero elements of the quasi-kernel and the elements of F_d, the distributive elements of F.

Theorem 2.2.52. *Let* (F, F) *be a near-vector space where* F *is a finite Dickson near-field and the scalar multiplication is the multiplication of* F. *Then* $(V, +, \mathcal{F})$ *is a fibered group where* $\mathcal{F} = \{bF_d | b \in Q(F)^*\}$.

Proof. Suppose F is a finite Dickson near-field and (F, F) is a near-vector space with scalar multiplication being the multiplication of F. Let $b \in Q(F)^*$ and $b\lambda_1, b\lambda_2 \in bF_d$, where $\lambda_1, \lambda_2 \in F_d$. We want to show that $(bF_d, +)$ is a subgroup of $(F, +)$. Since $0 \in F_d$, we have that $0 \in bF_d$, and

$$\begin{aligned} b\lambda_1 - b\lambda_2 &= \lambda_1 b - \lambda_2 b \quad \text{since } F_d \text{ is the center of } F, \\ &= (\lambda_1 - \lambda_2)b \\ &= b(\lambda_1 - \lambda_2) \quad \text{since } \lambda_1 - \lambda_2 \in F_d. \end{aligned}$$

Thus, $(bF_d, +)$ is a subgroup of $(F, +)$. Since F_d defines a group action on F, and by Lemma 2.2.50, $Q(F) = F$, we have that $F = \bigcup_{b \in Q(F)^*} bF_d$. □

2.3 Graph Theory

Graph theory can be used as a tool to graphically represent algebraic structures and their properties, e.g. [2] and [12]. Later in this thesis we will use the theory below to graphically represent some properties of near-vector spaces.

We will start with the definition of a graph.

Definition 2.3.1. *A graph G is a finite non-empty set $Z(G)$ of objects called vertices, together with a (possibly empty) set $E(G)$ of pairs of distinct vertices of G called edges. G can be written $G = (Z, E)$, to indicate that the graph G has a vertex set Z and edge set E.*

If $\{u, v\} \in E(G)$ is an edge in G, it is usually denoted simply as $uv \in E(G)$ and the vertices u and v are said to be adjacent vertices, and they are thus neighbours of one another. Furthermore, a neighbourhood of a vertex v, $N(v)$, in a graph G is the set of all vertices adjacent to v.

A graph G that contains no edges is called an empty graph. A graph with only one vertex is called a trivial graph. In this thesis we consider only simple graphs, i.e. undirected and without loops or multiple edges.

Definition 2.3.2. *A graph G is said to have order n and size m, where n represents the number of vertices of G, $|Z(G)|$, and m represents the number of edges of G, $|E(G)|$.*

The degree of vertex v, denoted $deg(v)$, is the order of the neighbourhood of v, $|N(v)|$. A vertex that is adjacent to every other vertex of the graph is called a universal vertex.

Definition 2.3.3. *A graph G_1 is said to be isomorphic to a graph G_2 if there exists a bijective function*

$$\phi : Z(G_1) \to Z(G_2)$$

such that $uv \in E(G_1)$ *if and only if* $\phi(u)\phi(v) \in E(G_2)$. *The function* ϕ *is called an isomorphism from* G_1 *to* G_2.

Next, we define what a subgraph of a graph is.

Definition 2.3.4. *A graph* H *is called a subgraph of a graph* G *if* $Z(H) \subseteq Z(G)$ *and* $E(H) \subseteq E(G)$. *To denote that* H *is a subgraph of* G *we write* $H \subseteq G$. *Furthermore, a graph* H *is called a proper subgraph of* G *if* H *is a subgraph of* G *and either* $Z(H)$ *or* $E(H)$ *is a proper subset of* $Z(G)$ *or* $E(G)$, *respectively.*

Let G be a graph. For $u, v \in Z(G)$, a $u - v$ walk W in G is a sequence of vertices and edges which starts with u and ends with v. Vertices and edges may be repeated in a walk. If no repetition of edges occur in a walk, then it is called a trail. Vertices may be repeated in a trail, and a trail that starts and ends with the same vertex is called a closed trail or a circuit. If no repetition of vertices occurs in a $u - v$ trail, then it is called a path. If the edge (v, u) is added to a $u - v$ path, then it is called a closed path or a cycle.

A graph G is connected if for every pair of vertices u and v in G there exists a $u - v$ path in G. A component in a graph G is a subgraph that is maximal with respect to the property of being connected. If a graph G is not connected, then G is said to be disconnected and it contains more than one component.

If G is a graph (connected or disconnected) and the removal of one of its vertices results in the number of components of G increasing, then that vertex is called a cut-vertex.

A graph G is said to be regular if every vertex $v \in Z(G)$ has the same degree. If that degree is r, then we call G r-regular. We now define a complete graph:

Definition 2.3.5. *A graph* G *of order* n *is said to be complete, denoted by* K_n, *if all vertices in* G *are adjacent to one another. Complete graphs of order* n *are* $(n-1)$*-regular and have size* $\binom{n}{2}$.

Example 2.3.6.
The following are examples of complete graphs:

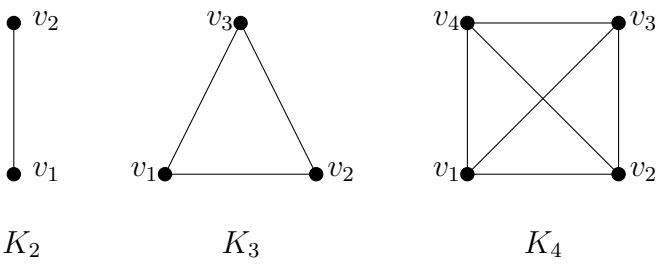


Figure 2.1: Complete graphs

$\Diamond$

In certain instances the vertex set $Z(G)$ of a graph G can be partitioned into sets, depending on the adjacency of the vertices.

Definition 2.3.7. *A graph G is said to be bipartite if the vertex set of G, $Z(G)$, can be partitioned into two (partite) sets such that every edge of G occurs only between vertices from distinct partite sets.*

Example 2.3.8.
Consider the graph G below:

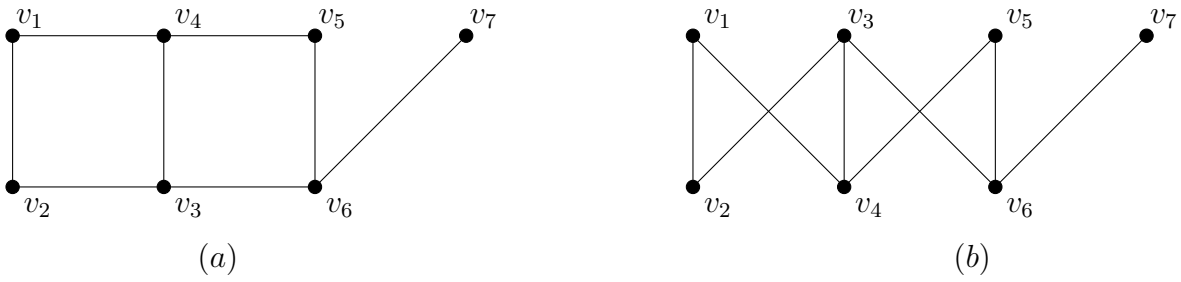


Figure 2.2: A bipartite graph G

The graph G being bipartite may be easily seen if we interchange the vertices v_3 and v_4 while retaining their adjacency in (a) to obtain (b). Another means of determining whether a graph is bipartite, is if we use vertex colouring. The idea is to use a different colour every time we colour adjacent vertices, while keeping the number of different colours to a minimum. If we choose colour 1 for a vertex, say v_1, and choose a different colour, say colour 2, for vertices adjacent to v_1, then we can use the colour 2 for vertices v_2 and

v_4, since neither of them are adjacent to one another. We can use colour 1 again for v_3, since it is not adjacent to v_1. If we continue in this manner, we will find that 2 colours are sufficient, hence our vertices can be partitioned into 2 sets. ◊

The following result can be found in [14].

Theorem 2.3.9. *A non-trivial graph is bipartite if and only if it contains no odd cycles.*

In the example above, the graph G is not a complete bipartite graph, since it is not the case that every vertex in the one partite set is adjacent to every vertex in the other partite set. If k is the least number of partite sets in any partition of the vertex set $V(G)$ of the graph G such that all edges in G occur only between vertices in distinct partite sets, then G is said to be k-partite.

Example 2.3.10.
Referring to Example 2.3.8, the complete bipartite graph of (b) is given by

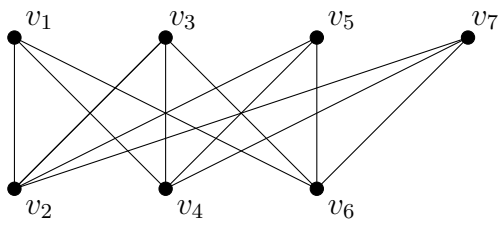


Figure 2.3: A complete bipartite graph $K_{4,3}$

◊

There are many ways in which one can produce a new graph from one or more given graphs. One of those ways is defined as follows:

Definition 2.3.11. *The complement $\overline{G}$ of a graph G is the graph with vertex set $Z(G)$ such that two vertices in $\overline{G}$ are adjacent if and only if they are not adjacent in G.*

For further reading, we direct the reader to [6] and [14].

Chapter 3

Near-vector space graphs and constructions

3.1 Introduction

In this section we focus on some near-vector space graphs and constructions. In Section 3.2 we look at the regularity and fibration graphs of near-vector spaces. Finally, in Section 3.3 we look at constructions of near-vector spaces. We begin with the direct sum of subspaces and end with quotient spaces.

3.2 Some graphs of near-vector spaces

3.2.1 The regularity graph

As remarked before, regularity is central in the theory of near-vector spaces. In [12] the regularity graph of a near-vector space was defined. This graph allows us to have a visual representation of the regularity of a near-vector space.

Definition 3.2.1. *([12]) Let (V, F) be a near-vector space and let $Z(V)$ be $Q(V)^* = Q(V) \setminus \{0\}$. The regularity graph of V, denoted $\Gamma(V)$, is the graph with vertices $Z(V)$ and edges ab if and only if a and b are compatible.*

Isomorphisms preserve regularity graphs:

Theorem 3.2.2. *([12]) If (V_1, F_1) and (V_2, F_2) are isomorphic near-vector spaces, then $\Gamma(V_1) \cong \Gamma(V_2)$.*

We focus on the construction discussed in Section 2.2.1. Thus we let $V = F^m$, $m \in \mathbb{N}$, where F is a finite Dickson near-field and ψ is the identity automorphism. In other words,

we have that for all $(x_1, x_2, \ldots, x_m) \in V$ and $\alpha \in F$,

$$(x_1, x_2, \ldots, x_m)\alpha = (x_1\alpha, x_2\alpha, \ldots, x_m\alpha).$$

Since for this construction, V is always regular, we have that:

Proposition 3.2.3. *([12]) For $V = F^m$, $m \in \mathbb{N}$, F a finite Dickson near-field and ψ the identity automorphism, $\Gamma(V) = K_{|Q(V)^*|}$.*

If F is a finite field, then (V, F) is a vector space and so it is clear that:

Lemma 3.2.4. *([12]) Let $V = F^m$, where F is a finite field and ψ the identity automorphism, then V is a vector space over F and*

$$\Gamma(V) = K_{|F|^m - 1}.$$

From Proposition 3.2.3 it is clear that in order to better describe the regularity graph in the case where F is a finite Dickson near-field, we need a formula for the cardinality of $Q(V)^*$. The first theorem below holds for a particular sub-class of finite Dickson near-fields, i.e. those where the Dickson pair (q, n) has the form $q = p$.

Theorem 3.2.5. *([12]) For the near-vector space (V, F), where $V = F^m$ and $F = DF(p, n)$ a finite Dickson near-field with the scalar multiplication defined for all $(x_1, \ldots, x_m) \in V, \alpha \in F$ by*

$$(x_1, \ldots, x_m)\alpha = (x_1\alpha, \ldots, x_m\alpha),$$

we have that

$$|Q(V)| = \frac{p^m - 1}{p - 1}(p^n - 1) + 1.$$

However, in [28], the above result was extended to all finite Dickson near-fields, that is, $q = p^l$ for $l \geq 1$.

Theorem 3.2.6. *([28]) Let $V = F^m$ be a regular near-vector space over a finite near-field $F = DF(q, n)$ with scalar multiplication defined for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$ by*

$$(x_1, \ldots, x_m)\alpha = (x_1\alpha, \ldots, x_m\alpha),$$

such that $|F_d| = q$ for some prime power q. Then

$$|Q(V)| = \frac{q^m - 1}{q - 1}(q^n - 1) + 1.$$

We can now describe the regularity graph for the construction under consideration.

Proposition 3.2.7. *Let $V = F^m$, where F is the finite Dickson near-field associated with the pair of Dickson numbers (q, n). Then*

$$\Gamma(V) = K_{\frac{q^m-1}{q-1}(q^n-1)}.$$

Example 3.2.8. *([12])*
Referring back to Example 2.2.35, let (V, F) be a near-vector space, with $V = F^3$ and $F = DF(3, 2)$. Suppose the scalar multiplication is defined for all $(x, y, z) \in V$ and $\alpha \in F$ by

$$(x, y, z)\alpha = (x\alpha, y\alpha, z\alpha).$$

The cardinality of $Q(V)$ using Theorem 3.2.6 is

$$\begin{aligned} |Q(V)| &= \frac{3^3-1}{3-1}(3^2-1)+1 \\ &= 105. \end{aligned}$$

Thus $\Gamma(V) = K_{104}$. ◊

We now move further away from traditional vector spaces and consider near-vector spaces where the multiplicative automorphisms are not all the identity.

In this case V is not necessarily regular. Let the canonical decomposition of V into maximal regular subspaces be given by $V = V_1 \oplus \cdots \oplus V_k$ and $m_1, \ldots, m_k$ be the dimensions of $V_1, \ldots, V_k$, respectively.

Theorem 3.2.9. *([12]) For the near-vector space (V, F), where $V = F^m, F = DF(p, n)$, the proper Dickson near-field of p^n elements and scalar multiplication is defined for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$ by*

$$(x_1, \ldots, x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the $\psi_i's$ are automorphisms of $(F, \cdot)$, for $i \in \{1, \ldots m\}$, we have that

$$\begin{aligned} |Q(V)| &= |Q(V_1)^*| + \ldots + |Q(V_k)^*| + 1 \\ &= \frac{p^{m_1}-1}{p-1}(p^n-1) + \ldots + \frac{p^{m_k}-1}{p-1}(p^n-1) + 1 \\ &= \frac{p^{m_1}+\cdots+p^{m_k}-k}{p-1}(p^n-1) + 1. \end{aligned}$$

As before, the above statement was generalised in [28] for all finite Dickson near-fields.

Theorem 3.2.10. *([28]) Let V be an m-dimensional near-vector space over a finite near-field $F = DF(q, n)$ such that $|F_d| = q$ for some prime power q and $|F| = q^n$. Let*

$V = \bigoplus_{i=1}^{k} V_i$ be the canonical decomposition of V with $dim(V_i) = m_i$ for $i \in \{1, \dots k\}$. Then

$$\begin{aligned} |Q(V)| &= |Q(V_1)^*| + \ldots + |Q(V_k)^*| + 1 \\ &= \frac{q^{m_1} - 1}{q - 1}(q^n - 1) + \ldots + \frac{q^{m_k - 1}}{q - 1}(q^n - 1) + 1 \\ &= \frac{q^{m_1} + \cdots + q^{m_k} - k}{q - 1}(q^n - 1) + 1. \end{aligned}$$

Proposition 3.2.11. *([12]) Let $V = F^m$ where $F = DF(p, n)$ is a finite Dickson near-field for (p, n) a Dickson pair, where p is prime. If we consider the near-vector space (V, F) where $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$, is the canonical decomposition of V, $\Gamma(V_i) = K_{\alpha_i}$, where*

$$\alpha_i = \frac{p^{m_i} - 1}{p - 1}(p^n - 1),$$

for $i = \{1, \dots, k\}$.

From Proposition 3.2.11 we have

Theorem 3.2.12. *([12]) Let $V = F^m$ where $F = DF(p, n)$ is a finite Dickson near-field for (p, n) a Dickson pair, where p is prime. If we consider the near-vector space (V, F), $\Gamma(V) = K_{\alpha_1} \cup \cdots \cup K_{\alpha_k}$, where*

$$\alpha_i = \frac{p^{m_i} - 1}{p - 1}(p^n - 1),$$

for $i = \{1, \dots, k\}$.

It is clear that:

Proposition 3.2.13. *([12]) The graph $\Gamma(V)$ has exactly k components, where k is the number of maximal regular subspaces in the canonical decomposition of V.*

To illustrate the above proposition and theorem, let us consider the following example.

Example 3.2.14.
Referring to Example 2.2.48 where $V = F^3$, $F = DF(3, 2)$. For the near-vector space (V, F), we have

$$\Gamma(V) = K_{32} \cup K_8,$$

where $|Q(V_1)^*| = \left(\frac{3^2 - 1}{3 - 1}\right)(3^2 - 1) = 32$ *and* $|Q(V_2)^*| = \left(\frac{3^1 - 1}{3 - 1}\right)(3^2 - 1) = 8.$ $\Diamond$

We generalise Proposition 3.2.11 and Theorem 3.2.12 for a finite Dickson near-field $DF(q, n)$.

Proposition 3.2.15. *Let $V = F^m$ be a non-regular near-vector space over $F = DF(q,n)$. If $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ is the canonical decomposition of V, then $\Gamma(V_i) = K_{\alpha_i}$, where*

$$\alpha_i = \frac{q^{m_i} - 1}{q - 1}(q^n - 1),$$

for $i = \{1, \ldots, k\}$.

Theorem 3.2.16. *Let (V, F) be a non-regular near-vector space, where $V = F^m$ and $F = DF(q,n)$. If $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ is the canonical decomposition of V, then $\Gamma(V) = K_{\alpha_1} \cup \cdots \cup K_{\alpha_k}$, where*

$$\alpha_i = \frac{q^{m_i} - 1}{q - 1}(q^n - 1),$$

for $i = \{1, \ldots, k\}$.

We close this section with some category theory as in [12]; however, we let $\mathcal{V}$ be the category of finite-dimensional near-vector spaces over a finite Dickson near-field $\mathrm{DF}(q,n)$ instead of $\mathrm{DF}(p,n)$.

Let $\mathcal{D}$ be the category of finite graphs which may have loops and multiple edges as objects and graph homomorphisms as morphisms. Recall that a function $\phi : Z(G) \to Z(H)$ is a homomorphism from a graph $G = (Z(G), E(G))$, with $Z(G)$ the set of vertices and $E(G)$ the set of edges, to a graph $H = (Z(H), E(H))$ if it preserves edges, i.e. for all edges $uv \in E(G)$, $\phi(u)\phi(v) \in E(H)$. Let $\mathcal{V}$ be the category of finite dimensional near-vector spaces over a finite Dickson near-field $\mathrm{DF}(q,n)$. Let γ be the mapping that assigns to every near-vector space (V, F) its regularity graph $\Gamma(V)$ and suppose that γ maps every linear mapping to the restriction of that linear mapping to $Q(V)^*$. This is a correction to the original result in [12], where γ mapped a linear mapping to itself. Then we can show that:

Proposition 3.2.17. *([12]) γ is a covariant functor from category $\mathcal{V}$ to $\mathcal{D}$.*

Proof. γ maps a near-vector space (V, F) in $\mathcal{V}$ to the graph $\Gamma(V)$ as defined above. Now let $f : (V_1, F) \to (V_2, F)$ be a linear mapping from the near-vector space (V_1, F) to the near-vector space (V_2, F). If $uv \in E(\Gamma(V_1))$, then by Proposition 2.2.23, $f(u)f(v) \in E(\Gamma(V_2)$ and so $\gamma(f) = f$ is a graph homomorphism from $\Gamma(V_1)$ to $\Gamma(V_2)$. So γ is well-defined. Also we have $\gamma(f \circ g) = f \circ g = \gamma(f) \circ \gamma(g)$ and $\gamma(1_{(V,F)}) = 1_{\Gamma(V)}$, for all composable linear maps f and g and near-vector spaces (V, F). Therefore γ is a covariant functor. □

The category $\mathcal{V}$ has a subcategory $\mathcal{R}$ consisting of all regular near-vector spaces over F as the set of objects and the linear mappings between them as the set of morphisms. This is a full subcategory of $\mathcal{V}$, since for all regular near-vector spaces (V_1, F) and (V_2, F) we

have $\mathcal{M}or_{\mathcal{R}}(V_1, V_2) = \mathcal{M}or_{\mathcal{V}}(V_1, V_2)$, where $\mathcal{M}or_{\mathcal{R}}(V_1, V_2)$ is the set of all linear mappings from V_1 to V_2 in the category $\mathcal{R}$. Also the category of all complete graphs together with graph morphisms between them is a full subcategory of $\mathcal{D}$. We denote it by $\mathcal{E}$. One may think that the restriction of γ from $\mathcal{R}$ to $\mathcal{E}$ is an equivalence of categories. But this is not the case. In fact γ is just faithful. But γ is neither full nor essentially surjective. We prove it in the following proposition.

Proposition 3.2.18. *([12]) The restriction of γ from $\mathcal{R}$ to $\mathcal{E}$ is a faithful functor but not essentially surjective and full.*

Proof. γ is faithful because $\gamma(f) = f$ for all f. We show that γ is not essentially surjective. γ will be essentially surjective if for a given complete graph Γ_t, it is always possible to find a regular near-vector space $(V, F) \in \mathcal{R}$ such that $\gamma(V, F) = \Gamma(V)$ is isomorphic to Γ_t. So we should have $|Z(\Gamma_t)| = |Q(V)^*| = t$, and so for any positive integer t we should be able to find a near-vector space such that $|Q(V)^*| = t$. But this is not true in general. Using Theorem 3.2.5, the cardinality of the quasi-kernel of any regular near-vector space V in $\mathcal{R}$ is of the form

$$|Q(V)| = \frac{q^n - 1}{q - 1}(q^m - 1) + 1,$$

with (q, n) a pair of Dickson numbers. $|Q(V)^*|$ cannot be 9, for example, and there are many other such examples. Thus we cannot find a near-vector space (V, F) such that its regularity graph is isomorphic to K_9, the complete graph of order 9. Therefore the restriction of γ from $\mathcal{R}$ to $\mathcal{E}$ is not essentially surjective. To show that it is not full, we use the fact that any set function from $Z(K_n)$ to $Z(K_m)$, where K_n and K_m are complete graphs, is a graph homomorphism from K_n to K_m. Since both are complete graphs, if $f : Z(K_n) \to Z(K_m)$ is any set function then we have for all $xy \in E(K_n)$, $f(x)f(y) \in E(K_m)$. But it is not true in general that every function between regular near-vector spaces is a linear mapping. So for regular near-vector spaces $(V_1, F), (V_2, F)$, we have in general $\mathcal{M}or_{\mathcal{R}}((V_1, F), (V_2, F)) \subsetneq \mathcal{M}or_{\mathcal{R}}(\Gamma(V_1), \Gamma(V_2))$. Hence γ is not full. □

Theorem 3.2.19. *([12]) There are no subcategories $\mathcal{V}_1$ of $\mathcal{V}$ and $\mathcal{D}_1$ of $\mathcal{D}$ such that γ is an equivalence from $\mathcal{V}_1$ to $\mathcal{D}_1$.*

Proof. Let's suppose that there are subcategories $\mathcal{D}_1$ of $\mathcal{D}$ and $\mathcal{V}_1$ of $\mathcal{V}$ such that γ is an equivalence from $\mathcal{V}_1$ to $\mathcal{D}_1$. We show that γ is not full and this will prove that γ cannot be an equivalence. Let (V, F) be an object of $\mathcal{V}_1$ and let $V = V_1 \oplus \cdots \oplus V_r$ be its canonical decomposition. Then the regularity graph, $\gamma((V, F))$, is of the form $K_{n_1} \cup \cdots \cup K_{n_r}$, where K_{n_i} is a complete graph for $i \in \{1, \ldots, r\}$. Since $\gamma(f) = f$, we should have $\mathcal{M}or_{\mathcal{V}_1}(V, V) = \mathcal{M}or_{\mathcal{D}_1}(\Gamma(V), \Gamma(V))$ assuming the fact that γ is full. But we see that any function $g : Z(\Gamma(V)) \to Z(\Gamma(V))$ satisfying $f(Z(K_{n_i})) \subset Z(K_{n_j})$, for $i, j \in \{1, \ldots, r\}$, is a graph homomorphism from $\Gamma(V)$ to $\Gamma(V)$, since the ${K_{n_i}}'s$ are complete graphs. So g should also be a linear mapping from (V, F) to itself. This is not true in general. So γ is not full. Therefore γ is not an equivalence from $\mathcal{V}_1$ to $\mathcal{D}_1$. □

3.2.2 The fibration graph

In this section we study the fibrations of near-vector spaces. Fibrations are important since they allow us to define some incidence structures for near-vector spaces, for example see [17].

We first define a graph to capture the equivalence relation $\asymp$ (Definition 2.2.29). Note that since $\asymp$ is an equivalence relation on V, it is one on $Q(V)$, thus we can define:

Definition 3.2.20. *For the near-vector space (V, A), we define the fibration graph $\Gamma_{\mathcal{F}}(V)$ of V as the graph with vertices $Z(V)$, the elements of $Q(V)^* = Q(V) \setminus \{0\}$ and edges ab if and only if $a \asymp b$ for $a, b \in Q(V)^*$.*

Isomorphisms preserve fibration graphs.

Proposition 3.2.21. *If (V_1, A_1) and (V_2, A_2) are isomorphic near-vector spaces, then $\Gamma_{\mathcal{A}_1}(V_1) \cong \Gamma_{\mathcal{A}_2}(V_2)$.*

Proof. Let (V_1, A_1) and (V_2, A_2) be isomorphic near-vector spaces. Suppose the isomorphism is (θ, η). Let

$$\begin{aligned} f : (Z(\Gamma_{A_1}(V_1)) &\to (Z(\Gamma_{A_2}(V_2)) \\ v &\mapsto \theta(v). \end{aligned}$$

Then f is one-to-one and by Proposition 2.2.27, $\theta(v) \in Q(V_2)$. Suppose $uv \in E(\Gamma_{\mathcal{A}_1}(V_1))$, then $u \asymp v$ and $v = u\lambda$ for some $\lambda \in A_1^*$. If $v \in V_1^*$, then by Definition 2.2.24 and Proposition 2.2.27 we have that

$$\begin{aligned} f(v) = \theta(v) &= \theta(u\lambda) \\ &= \theta(u)\eta(\lambda), \quad \text{with } \eta(\lambda) \in A_2^* \\ &= f(u)\eta(\lambda). \end{aligned}$$

Therefore, $f(u) \asymp f(v)$ and $f(u)f(v) \in E(\Gamma_{\mathcal{A}_2}(V_2))$, proving that f preserves adjacency. □

It is useful to note that by the definition of a near-vector space, A is a group action on V and the orbits for all $v \in V$ under A is given by

$$[v] = \{u \in V | u \asymp v\}.$$

A question that arises is, can we relate the above equivalence relation to $\sim$? Recall that $\sim$ is the equivalence relation defined on elements in $Q(V)^*$, where for $u, v \in Q(V)^*$, $u \sim v$ if and only if there exists a $\lambda \in A^*$ such that $u + v\lambda \in Q(V)$. The two equivalence relations $\sim$ and $\asymp$ are related in the following manner:

Lemma 3.2.22. *([17]) Let (V, A) be a near-vector space and $u, v \in Q(V)^*$ with $u \asymp v$, then $u \sim v$.*

While it is true that under certain conditions $\asymp$ implies $\sim$ (see [17]), the converse is not true. We illustrate this with a counter-example.

Example 3.2.23. *Let (V, F) be a near-vector space, where $V = (\mathbb{Z}_5)^4$ and $F = \mathbb{Z}_5$, and scalar multiplication is defined for all $(x_1, x_2, x_3, x_4) \in V$ and $\alpha \in F$ by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3).$$

V is not regular and the canonical decomposition of V is given by $V = V_1 \oplus V_2$, where $V_i = Q_i$ for $i \in \{1, 2\}$ is given by

$$V_1 = \{(a, 0, c, 0) | a, c \in F\}$$
$$V_2 = \{(0, b, 0, d) | b, d \in F\}.$$

Let $u, v \in Q(V)$, where $u = (1, 0, 2, 0)$ and $v = (1, 0, 3, 0)$. Then $u \sim v$ since there exists a $\lambda \in F^*$ such that $u + v\lambda \in Q(V)$, but no such $\lambda' \in F^*$ such that $u = v\lambda'$. Hence $\sim$ does not imply $\asymp$. ◊

For the rest of this section we focus on near-vector spaces, (V, F), where $V = F^m$ and $F = GF(p^r)$ is a finite field and scalar multiplication is defined for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$ by

$$(x_1, \ldots, x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha))$$

where the ψ_i's are automorphisms of $(F, \cdot)$. We focus on the first block construction in Section 2.2.1, i.e. A_i, where $i \in \{1, \ldots, k\}$, is a partition of $\{1, \ldots, m\}$ where $A_i = \{j \in I | \psi_i(\alpha) = \psi_j(\alpha^{p^l})$ for some $l \in \{0, \ldots, r-1\}\}$. By using Theorem 2.2.32, it was shown in [17] that these constructions are always fibered groups, or can be decomposed into fibered groups.

Theorem 3.2.24. *([17]) Any near-vector space (V, F), where $V = F^m$, with $F = GF(p^r)$ and scalar multiplication defined for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$ as*

$$(x_1, \ldots, x_m)\alpha := (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the $\psi_i's$ are automorphisms of $(F, \cdot)$ is a fibered group, or can be decomposed into fibered groups.

It is not difficult to show that:

Proposition 3.2.25. *For the near-vector space (V, F) where F is a finite field, each of the regular maximal near-vector spaces in the decomposition of V determines a fibration.*

Proof. There are two cases to consider.
Case 1: V is regular then by Theorem 2.2.46, $Q(V) = V$. V is then its own decomposition into maximal regular subspaces and by Theorem 2.2.32, there will be one fibration, namely $\mathcal{F} = \{bA | b \in Q(V)^*\}$.

Case 2: V is not regular, then by Lemma 2.2.44 it decomposes into maximal regular subspaces, say $V = V_1 \oplus \cdots \oplus V_k$ for some $k \in \mathbb{N}$, where by Theorem 2.2.46, $Q(V_i) = V_i$ for each $i \in \{1, \ldots, k\}$. By Theorem 2.2.32 each of these is a fibered group, thus there will be k of them. □

Finally, it can be shown when the fibers and the maximal subspaces of a near-vector space coincide.

Theorem 3.2.26. *([17]) Let $F = GF(p^r)$ and $V = F^m$ be a near-vector space with scalar multiplication defined for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$ by*

$$(x_1, \ldots, x_m)\alpha := (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the ψ_i's are automorphisms of $(F, \cdot)$ and for all $i, j \in I$ and $\alpha \in GF(p^r)$, $\psi_i(\alpha) \neq \psi_j(\alpha^{p^l})$, for any $l \in \{0, \ldots, r-1\}$, then $(V, \mathcal{F})$ is a fibration where the fibers are the maximal regular subspaces in the canonical decomposition of V.

This allows us to link the regularity and fibration graphs.

Theorem 3.2.27. *For the near-vector space construction defined in Theorem 3.2.26 we have that*

$$\Gamma_{\mathcal{F}}(V) \cong \Gamma(V).$$

Proof. Define

$$\begin{aligned} g : Z(\Gamma_{\mathcal{F}}(V)) &\to Z(\Gamma(V)) \\ v &\to v, \text{ i.e. the identity map} \end{aligned}$$

Then g is one-to-one since $Z(\Gamma_{\mathcal{F}}(V)) = Z(\Gamma(V))$. Now suppose that $uv \in E(\Gamma_{\mathcal{F}}(V))$, then $v = u\lambda_1$, for $\lambda_1 \in F^*$ and u and v belong to the same $\mathcal{F}_i$ for some $i \in \{1, \ldots, n\}$. But this implies, by Theorem 3.2.26, that u and v belong to the same maximal regular subspace V_i, for $i \in \{1, \ldots, k\}$. Thus $g(u)g(v) \in E(\Gamma(V))$ and $\Gamma_{\mathcal{F}}(V) \cong \Gamma(V)$.
Furthermore, we need to show that g^{-1} is a graph homomorphism. Since g is one-to-one, the inverse of g exists. But by Lemma 3.2.22, we have that $u \asymp v$ implies $u \sim v$ for $u, v \in Q(V)^*$. In other words, $uv \in E(\Gamma_{\mathcal{F}}(V))$ implies that $uv \in E(\Gamma(V))$. We then have that $g^{-1}(uv) = uv = g^{-1}(u)g^{-1}(v)$. □

For results 3.2.28 to 3.2.31 we return to the near-vector space with scalar multiplication defined for all $(x_1, \ldots, x_m) \in V$ and all $\alpha \in F$ by

$$(x_1, \ldots, x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the ψ_i's are automorphisms of $(F, \cdot)$ for all $i \in I$.

We have already remarked that in general, V being regular does not imply that $Q(V) = V$. But for finite field constructions, it turns out that the two are equivalent (see Theorem 2.2.46).

We use this to prove the following result.

Proposition 3.2.28. *Let $F = GF(p^r)$ and (V, F) be a near-vector space. Then the fibration graph $\Gamma_{\mathcal{F}}(V)$ is a subgraph of the regularity graph $\Gamma(V)$.*

Proof. We have that $Z(\Gamma_{\mathcal{F}}(V)) = Z(\Gamma(V))$ and by Lemma 3.2.4 if $u \asymp v$, i.e. $uv \in E(\Gamma_{\mathcal{F}}(V))$ then $u \sim v$, i.e. $uv \in E(\Gamma(V))$. Thus $\Gamma_{\mathcal{F}}(V)$ is a subgraph of $\Gamma(V)$. □

Remark 3.2.29.
We note that if (V, F) is regular, we have that $|P(V)| = \dfrac{p^{rm} - 1}{p^r - 1}$ (see [17]). In fact, we can link this with the cardinality of $Q(V)$. Since in this case $Q(V) = V$, we have that $|V| = |P(V)|(p^r - 1) + 1 = |Q(V)|$.

We can now show that:

Theorem 3.2.30. *If (V, F) is a near-vector space where F is a finite field, then*
(1) if $Q(V) = V$, then $\Gamma_{\mathcal{F}}(V) = \bigcup_{j=1}^{|P(V)|} K_{|F^*|}$;
(2) if $Q(V) \neq V$, then $\Gamma_{\mathcal{F}}(V) = \bigcup_{i=1}^{k} \Gamma_{\mathcal{F}_i}(V_i)$, where $\Gamma_{\mathcal{F}_i}(V_i) = \bigcup_{j=1}^{|P(V_i)|} K_{|F^*|}$.

Proof.
1. Suppose $Q(V) = V$, then by Theorem 3.2.24, $(V, +, \mathcal{F})$ is a fibered group where $\mathcal{F} = \{aF | a \in Q(V)^*\}$. It follows that the fibration graph will be the union of complete graphs each representing a fiber, up to the number of equivalence classes, $|P(V)|$.
2. Suppose $Q(V) \neq V$, then by Theorem 2.2.18, V can be decomposed into maximal regular near-vector spaces V_i, $i \in \{1, \ldots, k\}$, where since F is a field, by Lemma 2.2.44, $Q(V_i) = V_i$. Then by Theorem 2.2.46 each (V_i, F) is a regular near-vector space and each $(V_i, \mathcal{F}_i)$ is a fibered group for $i \in \{1, \ldots, r\}$. Hence the fibration graph will be the union of all the complete graphs of each fiber of each fibration $\mathcal{F}_i$.

□

From this it is clear that:

Corollary 3.2.31. *If (V, F) is a near-vector space where F is a finite field, then*

1. *if $Q(V) = V$, $\Gamma_{\mathcal{F}}(V)$ has $|P(V)|$ components.*
2. *if $Q(V) \neq V$, $\Gamma_{\mathcal{F}}(V)$ has $\sum_{i=1}^{k} |P(V_i)|$ components.*

Example 3.2.32.
Refer to Example 2.2.43, with $F = GF(3^3)$ and $V = F^4$. Suppose for all $(x_1, x_2, x_3, x_4) \in V$ and all $\alpha \in F$, scalar multiplication is defined by

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^9).$$

Put $\psi_1(\alpha) = \alpha = \psi_3(\alpha)$, $\psi_2(\alpha) = \alpha^3$ and $\psi_4(\alpha) = \alpha^9$. Then

$$\begin{aligned} \psi_4(\alpha^3) &= (\alpha^3)^9 \\ &= \alpha^{27} \\ &= \alpha \ mod\ 26 \\ &= \psi_1(\alpha). \end{aligned}$$

Thus, by Lemma 2.2.41, V is regular. Thus $\mathcal{F} = \{aF | a \in V^*\}$. By Theorem 2.2.46, $Q(V) = V$ and so $|P(V)| = |\mathcal{F}|$, where $|P(V)| = \dfrac{3^{12} - 1}{3^3 - 1} = 20,440$. ◊

In the following example we look at a near-vector space which is not regular.

Example 3.2.33.
Refer to Example 2.2.45, where $V = (\mathbb{Z}_5)^4$ and $F = \mathbb{Z}_5$, and scalar multiplication is defined for all $(x_1, x_2, x_3, x_4) \in V$ and $\alpha \in F$ by

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3).$$

We have $V = V_1 \oplus V_2$ and $(V_i, \mathcal{F}_i)$ is a fibered group for $i \in \{1, 2\}$, where

$$\mathcal{F}_1 = \{\{(1,0,0,0)F\}, \{(0,0,1,0)F\}, \{(1,0,1,0)F\}, \{(1,0,2,0)F\}, \{(1,0,3,0)F\}, \{(1,0,4,0)F\}\}$$

and

$$\mathcal{F}_2 = \{\{(0,1,0,0)F\}, \{(0,0,0,1)F\}, \{(0,1,0,1)F\}, \{(0,1,0,2)F\}, \{(0,1,0,3)F\}, \{(0,1,0,4)F\}\}.$$

Thus $\Gamma_{\mathcal{F}}(V) = \Gamma_{\mathcal{F}_1}(V_1) \bigcup \Gamma_{\mathcal{F}_2}(V_2)$ where $\Gamma_{\mathcal{F}_1}(V_1) = \bigcup_{i=1}^{6} K_4$ and $\Gamma_{\mathcal{F}_2}(V) = \bigcup_{i=1}^{6} K_4$.

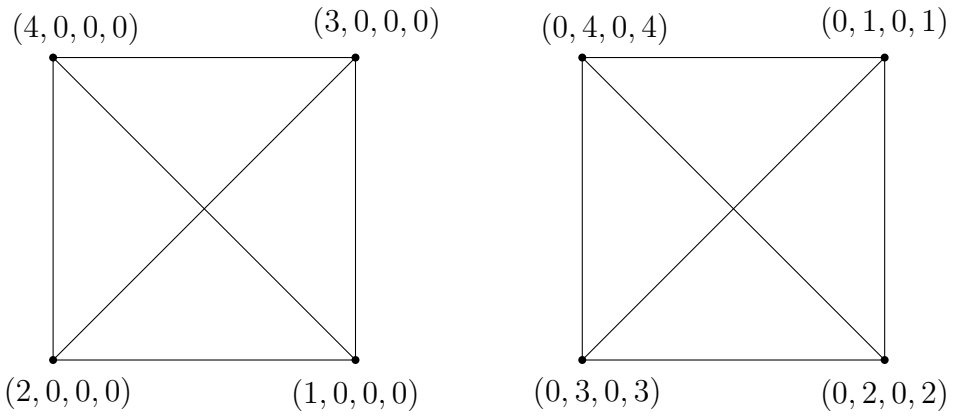


Figure 3.1: *K_4 graphs representing components in $\Gamma_{\mathcal{F}_1}(V_1)$ (left) and $\Gamma_{\mathcal{F}_2}(V_2)$*

◊

If we consider the construction (V, F) with $V = (\mathbb{Z}_p)^m$, we can say more. Since all the non-zero elements of $(\mathbb{Z}_p, +)$ are generators, we can form the set of all generators

$$S = \{g_i | i \in \{1, \ldots, p-1\}\} = \mathbb{Z}_p^*.$$

We can use this to completely describe the fibers in the case where V is not regular. We have a block construction where $A_i = \{b_1, b_2, \ldots, b_s\}$ for some $s \in \mathbb{N}$ is a cell in the partition of $\{1, \ldots, m\}$. We want to characterise the m-tuples used to generate each fiber of the near-vector space.

For ease of use, let 1 be fixed for the first non-zero component. Let g_{i_1} be the second non-zero component in the m-tuple, where g_{i_1}, $i_1 \in \{1, \ldots, p-1\}$ runs once through the entire set of elements of S, i.e. $p-1$ times. Then $(g_{i_1})_{i_2}$ denotes a component in the m-tuple where for each $g_{i_1} \in S$ in a preceding component, $(g_{i_1})_{i_2}$ will run through all elements of S $(p-1)$ times. In total, $(g_{i_1})_{i_2}$ will result in $(p-1)^2$ tuples. For each $(g_{i_1})_{i_2} \in S$ in a preceding component, $((g_{i_1})_{i_2})_{i_3}$ will denote a component in the m-tuple that will run through all elements of S $(p-1)$ times, and therefore result in $(p-1)^3$ tuples. The m-tuples will contain zeros in all the positions not labelled $b_1, b_2, \ldots, b_s$. Let the s-tuple denote the tuple after all the zero positions are removed from the m-tuples.

Proposition 3.2.34. *Let $V = F^m$ where $F = \mathbb{Z}_p$ and V is not regular. Let $A_i = \{b_1, b_2, \ldots, b_s\}$ be a cell in the partition of $\{1, \ldots, m\}$ as below Example 3.2.23, for $i \in \{1, \ldots, k\}$ and $S = \{g_1, g_2, \ldots, g_{p-1}\}$ be the set of generators, where $gcd(g_i, p) = 1$. Then the s-tuples (where $m - s$ zeros have been removed) of each of the k fibers will have the following form:*

- *e_j, where e_j has 1 in position j, for $j \in A_i$, $i \in \{1, \ldots, k\}$, and zeros elsewhere;*

- $(1, g_{i_1}, \ldots, 0)$, $(1, 0, g_{i_1}, \ldots, 0), \ldots (1, 0, \ldots, g_{i_1})$, $(0, 1, g_{i_1}, \ldots, 0), \ldots (0, 1, \ldots, g_{i_1}), \ldots$ $(0, \ldots, 1, g_{i_1})$, *where* $g_{i_1} \in S$ *and* $i_1 = \{1, \ldots, p-1\}$;
- $(1, g_{i_1}, (g_{i_1})_{i_2}, \ldots, 0)$, $(1, g_{i_1}, 0, (g_{i_1})_{i_2}, \ldots, 0), (1, g_{i_1}, \ldots, (g_{i_1})_{i_2}), \ldots (1, 0, g_{i_1}, \ldots, (g_{i_1})_{i_2})$, $\ldots (0, 1, g_{i_1}, (g_{i_1})_{i_2}, \ldots, 0), \ldots (0, 1, g_{i_1}, \ldots, (g_{i_1})_{i_2}), \ldots (0, \ldots, 1, g_{i_1}, (g_{i_1})_{i_2})$, *where* g_{i_1}, $(g_{i_1})_{i_2} \in S$ *and* $i_1, i_2 \in \{1, \ldots, p-1\}$;
  $\vdots$
- $(1, g_{i_1}, (g_{i_1})_{i_2}, \ldots, (((g_{i_1})_{i_2})_{i_3} \ldots)_{i_{s-1}})$, *where* $g_{i_1}, \ldots, (((g_{i_1})_{i_2})_{i_3} \ldots)_{i_l} \in S$, $l \in \{1, \ldots, s-1\}$ *and* $i_l = \{1, \ldots, p-1\}$.

The total number of s*-tuples is given by* $\dfrac{p^s - 1}{p-1}$.

Proof. We start with the least number of nonzero entries up until the most. The s-tuple e_j, with 1 in position j, where $j \in \{1, \ldots, s\}$, and zeros everywhere else, will give us the generating tuples for one non-zero entry and there will be s of them, that is $|e_j| = \binom{s}{1} = s$. Moving to two nonzero components, we must choose two of the components of the s-tuple to be non-zero; and for each of these choices, the first component must be 1 while the other can be any of the $p-1$ elements in S. There will be $\binom{s}{2}(p-1)$ of these.
For three non-zero components, we must choose two of the components of the s-tuple to be non-zero; and for each of these choices, the first component must be 1 while the other two can be any of the $p-1$ elements in S. The first of these two components, g_{i_1}, will run through the elements of S, and for each of the elements of S in this component, the second will run through each of the $p-1$ elements in S. There will be $\binom{s}{3}(p-1)^2$ of these. We continue in this manner until we reach s nonzero entries and we have one fixed entry as 1 and $s-1$ entries that run through each generator. There will be $\binom{s}{s}(p-1)^{s-1}$ of these. The total number of s-tuples above equals

$$\binom{s}{1} + \binom{s}{2}(p-1) + \binom{s}{3}(p-1)^2 + \ldots + \binom{s}{s}(p-1)^{s-1},$$

which comes to $\dfrac{(1 + (p-1))^s - 1}{p-1} = \dfrac{p^s - 1}{p-1}$. □

Remark 3.2.35.
The total number of s*-tuples correspond to the cardinality of the pseudo-projective space* $|P(V_i)|$, $i \in \{1, \ldots, k\}$, *of the maximal regular subspace* V_i, *as it should by Remark 3.2.29.*

We illustrate the result with an example.

Example 3.2.36.
Let $V = (\mathbb{Z}_5)^6$ where $F = \mathbb{Z}_5$ and suppose we are given that $A_1 = \{1, 3, 5, 6\}$ and $A_2 = \{2, 4\}$ gives the partition of $\{1, \ldots, 6\}$. If we want to list all the generating 4-tuples of $\mathcal{F}_1$, where we remove the zeros of the second and fourth component, we get the following.

- $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$, *and* $(0,0,0,1)$;
- $(1,1,0,0)$, $(1,0,1,0)$, $(1,0,0,1)$, $(0,1,1,0)$, $(0,1,0,1)$, $(0,0,1,1)$,
  $(1,2,0,0)$, $(1,0,2,0)$, $(1,0,0,2)$, $(0,1,2,0)$, $(0,1,0,2)$, $(0,0,1,2)$,
  $(1,3,0,0)$, $(1,0,3,0)$, $(1,0,0,3)$, $(0,1,3,0)$, $(0,1,0,3)$, $(0,0,1,3)$,
  $(1,4,0,0)$, $(1,0,4,0)$, $(1,0,0,4)$, $(0,1,4,0)$, $(0,1,0,4)$, *and* $(0,0,1,4)$;
- $(1,1,1,0)$, $(1,1,0,1)$, $(1,0,1,1)$, $(0,1,1,1)$
  $(1,1,2,0)$, $(1,1,0,2)$, $(1,0,1,2)$, $(0,1,1,2)$
  $(1,1,3,0)$, $(1,1,0,3)$, $(1,0,1,3)$, $(0,1,1,3)$
  $(1,1,4,0)$, $(1,1,0,4)$, $(1,0,1,4)$, $(0,1,1,4)$
  $(1,2,1,0)$, $(1,2,0,1)$, $(1,0,2,1)$, $(0,1,2,1)$
  $(1,2,2,0)$, $(1,2,0,2)$, $(1,0,2,2)$, $(0,1,2,2)$
  $(1,2,3,0)$, $(1,2,0,3)$, $(1,0,2,3)$, $(0,1,2,3)$
  $(1,2,4,0)$, $(1,2,0,4)$, $(1,0,2,4)$, $(0,1,2,4)$
  $(1,3,1,0)$, $(1,3,0,1)$, $(1,0,3,1)$, $(0,1,3,1)$
  $(1,3,2,0)$, $(1,3,0,2)$, $(1,0,3,2)$, $(0,1,3,2)$
  $(1,3,3,0)$, $(1,3,0,3)$, $(1,0,3,3)$, $(0,1,3,3)$
  $(1,3,4,0)$, $(1,3,0,4)$, $(1,0,3,4)$, $(0,1,3,4)$
  $(1,4,1,0)$, $(1,4,0,1)$, $(1,0,4,1)$, $(0,1,4,1)$
  $(1,4,2,0)$, $(1,4,0,2)$, $(1,0,4,2)$, $(0,1,4,2)$
  $(1,4,3,0)$, $(1,4,0,3)$, $(1,0,4,3)$, $(0,1,4,3)$
  $(1,4,4,0)$, $(1,4,0,4)$, $(1,0,4,4)$, *and* $(0,1,4,4)$;
- $(1,1,1,1)$, $(1,1,1,2)$, $(1,1,1,3)$, $(1,1,1,4)$
  $(1,1,2,1)$, $(1,1,2,2)$, $(1,1,2,3)$, $(1,1,2,4)$
  $(1,1,3,1)$, $(1,1,3,2)$, $(1,1,3,3)$, $(1,1,3,4)$
  $(1,1,4,1)$, $(1,1,4,2)$, $(1,1,4,3)$, $(1,1,4,4)$
  $(1,2,1,1)$, $(1,2,1,2)$, $(1,2,1,3)$, $(1,2,1,4)$
  $(1,2,2,1)$, $(1,2,2,2)$, $(1,2,2,3)$, $(1,2,2,4)$
  $(1,2,3,1)$, $(1,2,3,2)$, $(1,2,3,3)$, $(1,2,3,4)$
  $(1,2,4,1)$, $(1,2,4,2)$, $(1,2,4,3)$, $(1,2,4,4)$
  $(1,3,1,1)$, $(1,3,1,2)$, $(1,3,1,3)$, $(1,3,1,4)$
  $(1,3,2,1)$, $(1,3,2,2)$, $(1,3,2,3)$, $(1,3,2,4)$
  $(1,3,3,1)$, $(1,3,3,2)$, $(1,3,3,3)$, $(1,3,3,4)$
  $(1,3,4,1)$, $(1,3,4,2)$, $(1,3,4,3)$, $(1,3,4,4)$
  $(1,4,1,1)$, $(1,4,1,2)$, $(1,4,1,3)$, $(1,4,1,4)$
  $(1,4,2,1)$, $(1,4,2,2)$, $(1,4,2,3)$, $(1,4,2,4)$
  $(1,4,3,1)$, $(1,4,3,2)$, $(1,4,3,3)$, $(1,4,3,4)$

$(1,4,4,1)$, $(1,4,4,2)$, $(1,4,4,3)$, *and* $(1,4,4,4)$.

If we total the number of generating tuples for $\mathcal{F}_1$, *we get*

$$\begin{aligned}\frac{(1+(p-1))^s-1}{p-1} =& \frac{(5)^4-1}{4}\\ =& 156.\end{aligned}$$

Furthermore, the generating tuples for $\mathcal{F}_2$ *is given by* $(1,0)$, $(0,1)$ *and* $(1,1),(1,2),(1,3)$ *and* $(1,4)$. ◊

Remark 3.2.37.
We note that 1 can be replaced by any other generator as the fixed element.

As in the previous section, we will look at some category theory applicable to the fibration graphs. We define $\mathcal{V}_{\mathcal{F}}$ and $\mathcal{D}$ in a similar manner as the previous section, namely $\mathcal{D}$ is the category of finite graphs (with possible loops and multiple edges) as objects and graph homomorphisms as morphisms, and $\mathcal{V}_{\mathcal{F}}$ the category of finite dimensional near-vector spaces over a finite field F. However, in our case we define χ to be the mapping that assigns to every near-vector space (V,F) its fibration graph $\Gamma_{\mathcal{F}}(V)$ while χ maps every linear mapping to the restriction of that linear mapping to $Q(V)^*$.

Proposition 3.2.38. *The mapping* χ *is a covariant functor from category* $\mathcal{V}_{\mathcal{F}}$ *to* $\mathcal{D}$.

Proof. Define

$$\chi : \mathcal{V}_{\mathcal{F}} \Longrightarrow \mathcal{D}$$

with object part

$$\chi : obj(\mathcal{V}_{\mathcal{F}}) \to obj(\mathcal{D})$$

and arrow part

$$\chi : Mor(\mathcal{V}_{\mathcal{F}}) \quad \to \quad Mor(\mathcal{D})$$

Let $f : (V_1,F) \to (V_2,F)$ be a linear mapping from the near-vector space (V_1,F) to the near-vector space (V_2,F), where χ maps every linear mapping to the restriction of that linear mapping to $Q(V)^*$. We need to show that χ is well-defined, that the composition of morphisms is defined and the identity morphism exists.
Let $u,v \in Z(\Gamma_{\mathcal{F}}(V_1))$, then by Proposition 2.2.23, $f(u),f(v) \in Z(\Gamma_{\mathcal{F}}(V_2))$. If $uv \in E(\Gamma_{\mathcal{F}}(V_1))$, then $f(u)f(v) \in E(\Gamma_{\mathcal{F}}(V_2))$. Therefore, $\chi(f) = f$ is a graph homomorphism from $\Gamma_{\mathcal{F}}(V_1)$ to $\Gamma_{\mathcal{F}}(V_2)$, and distinct homomorphism sets are disjoint.
The composition of morphisms for all composable linear mappings f and g is given by

$$\begin{aligned}\chi(f \circ g) &= f \circ g\\ &= \chi(f) \circ \chi(g).\end{aligned}$$

And lastly, the identity map for all near-vector spaces (V, F) is given by

$$\chi(1_{(V,F)}) = 1_{\Gamma_{\mathcal{F}}(V)}.$$

□

The category $\mathcal{V}_{\mathcal{F}}$ has a subcategory $\mathcal{V}_Q$ consisting of all near-vector spaces over F with $Q(V) = V$ being the objects, and the linear mappings between them as the set of morphisms. $\mathcal{V}_Q$ is a full subcategory of $\mathcal{V}_{\mathcal{F}}$ since we have that the set $Mor_{\mathcal{V}_Q}(V_1, V_2)$ of all linear mappings from V_1 to V_2 in $\mathcal{V}_Q$ are exactly the set $Mor_{\mathcal{V}_{\mathcal{F}}}(V_1, V_2)$ of linear mappings from V_1 to V_2 in $\mathcal{V}_{\mathcal{F}}$. The category $\mathcal{D}$, in this case, has a full subcategory $\mathcal{E}'$ of the union of complete graphs with $|P(V)|$ components, and graph homomorphisms between them, as defined in the previous section.

If we look at the restriction of χ from $\mathcal{V}_Q$ to $\mathcal{E}'$, we also find that χ is faithful. For every near-vector space over F, where F is a field and where $Q(V) = V$, we can map it to a fibration graph, which is a union of complete graphs. This restriction of χ is also not full, as F is restricted by its prime power. We will prove it in the following proposition.

Proposition 3.2.39. *The restriction of χ from $\mathcal{V}_Q$ to $\mathcal{E}'$ is a faithful functor but not essentially surjective and full.*

Proof. To show that χ is faithful we show that the local arrow part of χ, that is, the restriction of χ to $Mor_{\mathcal{V}_Q}(V_1, V_2)$ is injective. Since $\chi(f) = f$ for all $f \in Mor_{\mathcal{V}_Q}(V_1, V_2)$ it follows that if $\chi(f) = \chi(g)$ then $f = g$ for any $g \in Mor_{\mathcal{V}_Q}(V_1, V_2)$.
To show that χ is not essentially surjective, we need to show that for any union of complete graphs E in $\mathcal{E}'$, we can find a near-vector space (V, F) in $\mathcal{V}_Q$ such that $\chi(V, F) = \Gamma_{\mathcal{F}}(V)$ is isomorphic to E. This implies that $|Z(\Gamma_{\mathcal{F}}(V))| = n|Q(V)^*| = n|P(V)|$, which is not always possible since $n = F^*$ is dependent on finding a suitable finite field, which comes with the restriction of a prime or prime power order. Therefore, the restriction of χ from $\mathcal{V}_Q$ to $\mathcal{E}'$ is not essentially surjective.
Lastly, we will show that χ is not full. We need to show that for every $f \in Mor(\Gamma_{\mathcal{F}}(V_1), \Gamma_{\mathcal{F}}(V_2))$ that is a graph homomorphism, we have that f is a linear mapping in $\mathcal{V}_Q$. Since $\Gamma_{\mathcal{F}}(V_1)$ and $\Gamma_{\mathcal{F}}(V_2)$ are both isomorphic to the union of complete graphs, we have that f is a homomorphism. However, not all f from (V_1, F) to (V_2, F) is necessarily a linear mapping, and therefore, χ is not full. □

Finally, we mention two graphs which were defined in [8] and [9] for vector spaces, namely the subspace sum- and subspace inclusion graphs. For the purposes of this thesis we will study the latter graph for near-vector space constructions over copies of finite fields.

3.2.3 Subspace Inclusion graph of a near-vector space

In [8] the inclusion graph $In(V_{vs})$ of a finite-dimensional vector space V_{vs} over a finite field F of dimension greater than 1 is defined as follows: let the vertices $Z(V_{vs})$ be the collection of proper non-trivial subspaces of V_{vs}, and for $W_1, W_2 \in Z(V_{vs})$, let the edges $E(V_{vs})$ of V_{vs} contain (W_1, W_2) if either $W_1 \subset W_2$ or $W_2 \subset W_1$. In other words, we have an edge between two proper non-trivial subspaces if one is contained in the other. Since the author requires that $dim(V_{vs}) > 1$ we have that $Z(V_{vs}) \neq \emptyset$. In addition, all vector spaces mentioned are finite-dimensional.
Throughout this section we will write GF(q) for the finite field of $q = p^r$ elements, where p is prime and $r \in \mathbb{Z}^+$. We will use "$\subset$" for proper containment.

We begin with a brief overview of the main results of [8]. The first result determines under what conditions $In(V_{vs})$ has a subgraph.

Theorem 3.2.40. *([8]) If V_{vs} is a vector space over a field F and W is a subspace of V_{vs} with dimension greater than 1, then $In(W)$ is a subgraph of $In(V_{vs})$.*

By the definition of $In(V_{vs})$, subspaces of the same dimension cannot have an edge between them. This is proven in the following lemma.

Lemma 3.2.41. *([8]) If W_1 and W_2 are two distinct subspaces of V_{vs} of the same dimension, then $(W_1, W_2) \notin E(V_{vs})$ in $In(V_{vs})$.*

It is also of interest to know when $In(V_{vs})$ will be an empty graph.

Corollary 3.2.42. *([8]) If $dim(V_{vs}) = 2$, then $In(V_{vs})$ is an edgeless graph.*

Finally, we have that $In(V_{vs})$ will never be a complete graph.

Corollary 3.2.43. *([8]) $In(V_{vs})$ is not complete.*

The author then studies properties of the inclusion graph where the vector space is constructed using copies of the finite field $F = GF(q)$. It is well-known that the number of t-dimensional non-trivial proper subspaces of an m-dimensional vector space is given by

$$\binom{m}{t}_q = \frac{(q^m - 1)(q^m - q)\dots(q^m - q^{t-1})}{(q^t - 1)(q^t - q)\dots(q^t - q^{t-1})}.$$

This formula was used to derive the following two results.

Proposition 3.2.44. *([8]) Let V_{vs} be an m-dimensional vector space over a finite field of order q. Then $In(V_{vs})$ is a graph of order*

$$\sum_{t=1}^{m-1} \binom{m}{t}_q.$$

The next result looks at the degree of any vertex of the inclusion graph of a vector space.

Theorem 3.2.45. *([8]) If W is a t-dimensional non-trivial proper subspace of V_{vs}, then $deg(W)$ in $In(V_{vs})$ is*

$$\sum_{i=1}^{t-1} \binom{t}{i}_q + \sum_{i=1}^{m-t-1} \binom{m-t}{i}_q.$$

We now define the subspace inclusion graph of a near-vector space.

Definition 3.2.46. *Let $V = F^m$ be a regular near-vector space over a field $F = GF(p^r)$. Then $\Gamma_{\mathcal{I}}(V) = (Z(V), E(V))$ denotes the subspace inclusion graph, where $Z(V)$ is the collection of nontrivial proper subspaces of V and for $W_1, W_2 \in Z(V)$,*

$$(W_1, W_2) \in E(V) \text{ if either } W_1 \subset W_2 \text{ or } W_2 \subset W_1.$$

It is not difficult to prove that:

Theorem 3.2.47. *If V is a near-vector space over a field F and W is a subspace of V with dimension greater than 1, then $\Gamma_{\mathcal{I}}(W)$ is a subgraph of $\Gamma_{\mathcal{I}}(V)$.*

Proof. If $\dim W > 1$, then by the definition of the subspace inclusion graph, $\Gamma_{\mathcal{I}}(W)$ exists. Since all subspaces of W are also subspaces of V, the result follows. □

In order to get a better feel for the inclusion graph, we need to first establish that near-vector spaces with the same dimension are isomorphic. We would like to credit Jacques Rabie for his input in the following result.

Corollary 3.2.48. *Let (V_1, F) and (V_2, F) be regular near-vector spaces over a finite field $F = GF(p^r)$. If $\dim V_1 = \dim V_2$, then $(V_1, F) \cong (V_2, F)$.*

Proof. Let (V_1, F) be the near-vector space, where $V_1 = F^m$ and $F = GF(p^r)$, such that scalar multiplication is defined for all $(x_1, \ldots, x_m) \in V_1$ and $\alpha \in F$ by

$$(x_1, \ldots, x_m)\alpha = (x_1\alpha^{q_1 p^{l_1}}, \ldots, x_m\alpha^{q_1 p^{l_m}})$$

and let (V_2, F) be the near-vector space, where $V_2 = F^m$ and $F = GF(p^r)$, such that scalar multiplication is defined for all $(x_1, \ldots, x_m) \in V_1$ and $\alpha \in F$ by

$$(x_1, \ldots, x_m)\alpha = (x_1\alpha^{q_2 p^{k_1}}, \ldots, x_m\alpha^{q_2 p^{k_m}}).$$

Define

$$\theta : V_1 \to V_2$$

by

$$(x_1, \ldots, x_n) \mapsto (x_1^{p^{k_1}/p^{l_1}}, \ldots, x_m^{p^{k_m}/p^{l_m}})$$

and

$$\eta : F \to F$$

by

$$\alpha \mapsto \alpha^{q_1/q_2}.$$

We want to show that θ and η are group homomorphisms. Let $s_i = k_i - l_i$, for $i \in \{1, \ldots, m\}$ and recall that $(x_1 + y_1)^{p^{s_1}} = x_1^{p^{s_1}} + y_1^{p^{s_1}}$ since F has characteristic p. For $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in V_1$, we have

$$\begin{aligned}
\theta((x_1, \ldots, x_m) + (y_1, \ldots, y_m)) &= \theta((x_1 + y_1, \ldots, x_m + y_m)) \\
&= ((x_1 + y_1)^{p^{s_1}}, \ldots, (x_m + y_m)^{p^{s_m}}) \\
&= (x_1^{p^{s_1}} + y_1^{p^{s_1}}, \ldots, x_m^{p^{s_m}} + y_m^{p^{s_m}}) \\
&= (x_1^{p^{s_1}}, \ldots, x_m^{p^{s_m}}) + (y_1^{p^{s_1}}, \ldots, y_m^{p^{s_m}}) \\
&= \theta((x_1, \ldots, x_m)) + \theta((y_1, \ldots, y_m))
\end{aligned}$$

and

$$\begin{aligned}
\eta(\alpha\beta) &= (\alpha\beta)^{q_1/q_2} \\
&= \alpha^{q_1/q_2}\beta^{q_1/q_2} \\
&= \eta(\alpha)\eta(\beta)
\end{aligned}$$

To show that θ and η are group isomorphisms, we show that for $ker(\theta) = \{(0, \ldots, 0)\}$ and $ker(\eta) = 1$, we get $(0, \ldots, 0)$ and 1, respectively. So for $(x_1, \ldots, x_m) \in V_1$,

$$\begin{aligned}
\theta((x_1, \ldots, x_m)) &= (0, \ldots, 0) \\
(x_1^{p^{k_1}/p^{l_1}}, \ldots, x_m^{p^{k_m}/p^{l_m}}) &= (0, \ldots, 0)
\end{aligned}$$

which implies that $x_i = 0$ for $i \in \{1, \ldots, m\}$, and $(x_1, \ldots, x_m) = (0, \ldots, 0)$. And for $\alpha \in F$,

$$\eta(\alpha) = 1$$
$$\alpha^{q_1/q_2} = 1.$$

By Lemma 2.4 in [20], every element if F has a q-th root in F if and only if $gcd(q, p^r - 1) = 1$. Therefore we get that

$$\alpha = 1.$$

Finally, we show that (θ, η) is an isomorphism. For $(x_1, \ldots, x_m) \in V_1$ and $\alpha \in F$,

$$\begin{aligned}
\theta((x_1, \ldots, x_m)\alpha) &= \theta((x_1\alpha^{q_1p^{l_1}}, \ldots, x_m\alpha^{q_1p^{l_m}})) \\
&= ((x_1\alpha^{q_1p^{l_1}})^{p^{k_1}/p^{l_1}}, \ldots, (x_m\alpha^{q_1p^{l_m}})^{p^{k_m}/p^{l_m}}) \\
&= (x_1^{p^{k_1}/p^{l_1}}\alpha^{q_1p^{k_1}}, \ldots, x_m^{p^{k_m}/p^{l_m}}\alpha^{q_1p^{k_m}}) \\
&= (x_1^{p^{k_1}/p^{l_1}}, \ldots, x_m^{p^{k_m}/p^{l_m}})\alpha^{q_1/q_2} \\
&= \theta(x_1, \ldots, x_m)\eta(\alpha).
\end{aligned}$$

Hence, (θ, η) is an isomorphism. □

Lemma 3.2.49. *If W_1 and W_2 are two distinct subspaces of a near-vector space $V = F^m$, where $F = GF(p^r)$, then $(W_1, W_2) \notin E(\Gamma_{\mathcal{I}}(V))$ if $\dim W_1 = \dim W_2$.*

Proof. Let W_1 and W_2 are non-trivial proper distinct t-dimensional subspaces of V. Let us suppose that $(W_1, W_2) \in E(\Gamma_{\mathcal{I}}(V))$, we will show that this leads to a contradiction. Then we have two cases: either (a) $W_1 \subset W_2$ or (b) $W_2 \subset W_1$. Without loss of generality, suppose that $W_1 \subset W_2$. By Lemma 2.2.8, we have that $Q(W_1) = W_1 \cap Q(W_2)$, which implies that $Q(W_1) \subset Q(W_2)$. This is a contradiction since W_1 and W_2 have the same dimension, which would imply that they have the same number of basis elements. Hence $(W_1, W_2) \notin E(\Gamma_{\mathcal{I}}(V))$. □

In addition, the following corollaries are not difficult to prove.

Corollary 3.2.50. *If $\dim V = 2$, then $\Gamma_{\mathcal{I}}(V)$ is an edgeless graph.*

Proof. Let $\dim V = 2$, then all the proper non-trivial subspaces have dimension 1. By Lemma 3.2.49, we have that none of these subspaces will be adjacent in $\Gamma_{\mathcal{I}}(V)$. □

Corollary 3.2.51. *$\Gamma_{\mathcal{I}}(V)$ is not complete.*

Proof. By definition, $\dim V > 1$. Therefore, there exists at least two linearly independent vectors $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in V$ such that the subspaces W_1, W_2 generated by these vectors, respectively, are not adjacent in $\Gamma_{\mathcal{I}}(V)$, i.e. $(W_1, W_2) \notin E(\Gamma_{\mathcal{I}}(V)$. □

Corollary 3.2.52. *Let V_1 and V_2 be two finite dimensional near-vector spaces over the same field F. If V_1 and V_2 are isomorphic, where (θ, η) is the isomorphism pair with η the identity mapping, then*

$$\Gamma_{\mathcal{I}}(V_1) \cong \Gamma_{\mathcal{I}}(V_2).$$

Proof. Suppose $(V_1, F) \cong (V_2, F)$, then there exists a pair (θ, η) such that

$$\begin{aligned} \theta : (V_1, +) &\to (V_2, +) \\ v_1 &\mapsto v_1' \end{aligned}$$

and

$$\eta : (F^*, \cdot) \to (F^*, \cdot)$$

where $\eta = id$. To prove that the inclusion graphs of V_1 and V_2 are isomorphic, we need to show that

(a) $|Z(\Gamma_{\mathcal{I}}(V_1))| = |Z(\Gamma_{\mathcal{I}}(V_2))|$; that is, subspaces are preserved, and

(b) if, for W_1 and W_2 non-empty, proper subspaces of V_1, $(W_1, W_2) \in E(\Gamma_{\mathcal{I}}(V_1))$, then $(\theta(W_1), \theta(W_2)) \in E(\Gamma_{\mathcal{I}}(V_2))$; that is, edges are preserved.

(a) We need to show that for any subspace, W_1, it's image will also be a subspace. By Corollary 2.2.12 , since F is a field and thus a division ring, we need to show that $\theta(W_1)$ is non-empty and closed under addition and scalar multiplication. We have that $0 \in W_1$, which means $\theta(0) \in \theta(W_1)$ and hence, $\theta(W_1)$ is non-empty. Furthermore, suppose that for $w_1,\ w_2 \in W_1$ and $\alpha, \beta \in F$, $w_1\alpha,\ w_2\beta \in W_1$. Then

$$\begin{aligned} \theta(w_1\alpha + w_2\beta) &= \theta(w_1\alpha) + \theta(w_2\beta) \\ &= \theta(w_1)\eta(\alpha) + \theta(w_2)\eta(\beta) \\ &= \theta(w_1)\alpha + \theta(w_2)\beta. \end{aligned}$$

Since $w_1\alpha + w_2\beta \in W_1$, we have that $\theta(w_1)\alpha + \theta(w_2)\beta \in \theta(W_1)$. Hence, $\theta(W_1)$ is closed under addition and scalar multiplication, and the non-empty, proper subspaces are preserved.

(b) We need to prove that if $W_1,\ W_2$ are non-empty, proper subspaces of V_1 and $W_1 \subset W_2$, then $\theta(W_1) \subset \theta(W_2)$. Let $\theta(w_1) \in \theta(W_1)$ then since $w_1 \in W_2$, $\theta(w_1) \in \theta(W_2)$. Hence, $\theta(W_1) \subset \theta(W_2)$.

□

The converse of the above corollary is not true. We could have that subspace inclusion graphs of near-vector spaces are isomorphic, but the near-vector spaces themselves are not isomorphic. Consider the next example:

Example 3.2.53. *Referring to Example 2.2.38, where $V = F^4$ is a near-vector space and $F = GF(3^3)$. By choosing (V_1, F) to be defined for all $(x_1, x_2, x_3, x_4) \in V_1$ and all $\alpha \in F$, by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha, x_3\alpha^5, x_4\alpha),$$

and (V_2, F) to be defined for all $(x_1, x_2, x_3, x_4) \in V_2$ and all $\alpha \in F$, by

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha, x_3\alpha^7, x_4\alpha),$$

we will obtain two near-vector spaces that are not isomorphic, but their subspace inclusion graphs will be isomorphic. ◊

We now state the result proven by S.P. Sanon for finding the number of t-dimensional subspaces of a near-vector space.

Theorem 3.2.54. *([28]) Let $V = F^m$ be a near-vector space over a finite near-field F with $|F_d| = q$ and $|F| = q^n$. Suppose V is regular, then the number of t-dimensional subspaces of V is given by the Gaussian binomial coefficient*

$$\binom{m}{t}_q = \frac{(q^m - 1)(q^m - q)\dots(q^m - q^{t-1})}{(q^t - 1)(q^t - q)\dots(q^t - q^{t-1})}.$$

The formula was derived from the number of different ways one can form a set of t linearly independent vectors taken from $Q(V)$. We illustrate the above with the following example.

Example 3.2.55. *Consider the regular near-vector space $V = F^5$ over finite field $F = \mathbb{Z}_5$, defined for all $(x_1, x_2, x_3, x_4, x_5) \in V$ and $\alpha \in F$ by*

$$(x_1, x_2, x_3, x_4, x_5)\alpha = (x_1\alpha^3, x_2\alpha^3, x_3\alpha^3, x_4\alpha, x_5\alpha).$$

The canonical decomposition of V is given by $V = V_1 \oplus V_2$, where $V_1 = \{(a, b, c, 0, 0) | a, b, c \in \mathbb{Z}_5\}$ and $V_2 = \{(0, 0, 0, d, e) | d, e \in \mathbb{Z}_5\}$. The number of 2-dimensional subspaces of V_1 is given by

$$\begin{aligned}\binom{3}{2}_5 &= \frac{(5^3 - 1)(5^3 - 5)}{(5^2 - 1)(5^2 - 5)} \\ &= \frac{(5^3 - 1)}{(5 - 1)} = \frac{124}{4} = 31\end{aligned}$$

The subspaces will have the form

(i) $W_i = \langle (1, 0, a, 0, 0), (0, 1, b, 0, 0) \rangle$ where $i \in \{1, 2, \dots, 25\}$ and $a, b \in \mathbb{Z}_5$;

(ii) $W_j = \langle (1, c, 0, 0, 0), (0, 0, 1, 0, 0) \rangle$ *where* $j \in \{26, \ldots, 30\}$ *and* $c \in \mathbb{Z}_5$*; and*

(iii) $W_{31} = \langle (0, 1, 0, 0, 0), (0, 0, 1, 0, 0) \rangle$.

Using the same formula as above, the number of 1-dimensional subspaces of V_1 *is also* 31*, and given by*

(i) $W_i' = \langle (1, a, b, 0, 0) \rangle$ *where* $i \in \{1, 2, \ldots, 25\}$ *and* $a, b \in \mathbb{Z}_5$*;*

(ii) $W_j' = \langle (0, 1, c, 0, 0) \rangle$ *where* $j \in \{26, \ldots, 30\}$ *and* $c \in \mathbb{Z}_5$*; and*

(iii) $W_{31}' = \langle (0, 0, 1, 0, 0) \rangle$.

$\Diamond$

In a regular near-vector space, every subspace will also be regular. In addition to this, no subspaces with the same dimension will be adjacent in the subspace inclusion graph. This leads us to the following theorem.

Theorem 3.2.56. *Let* $V = F^m$ *be a regular near-vector space over* $F = GF(q)$*. For all* $(x_1, \ldots, x_m) \in V$ *and* $\alpha \in F$*, define scalar multiplication by*

$$(x_1, \ldots, x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the ψ_i*'s are automorphisms of* $(F, \cdot)$*. Then the inclusion graph* $\Gamma_{\mathcal{I}}(V)$ *is an* $(m-1)$*-partite graph.*

Proof. The dimension of V is m, so then there are $\begin{pmatrix} m \\ t \end{pmatrix}_q$ distinct subspaces of dimension t, $t \in \{1, \ldots, m-1\}$. By Lemma 3.2.49, the subspaces of the same dimension are not adjacent in the subspace inclusion graph, hence these would form a set of non-adjacent subspaces for every t and there would be $m-1$ of them. Therefore, $\Gamma_{\mathcal{I}}(V)$ is an $(m-1)$-partite graph. $\square$

Next, we discuss the conditions for the existence of a subgraph of the inclusion graph of a near-vector space.

Theorem 3.2.57. *If* $V = F^m$ *is a regular near-vector space over a finite field* F*, and* W *is a proper subspace of* V *with* $\dim W > 1$*, then* $\Gamma_{\mathcal{I}}(W)$ *is a subgraph of* $\Gamma_{\mathcal{I}}(V)$*.*

Proof. Suppose that W is a proper subspace of V with $\dim W > 1$, then clearly $Z(W)$ is a subset of $Z(V)$. Moreover, since every subspace of W will be a subspace of V it follows that for every $(W_1, W_2) \in E(W)$ we have $(W_1, W_2) \in E(V)$. Therefore, $\Gamma_{\mathcal{I}}(W)$ is a subgraph of $\Gamma_{\mathcal{I}}(V)$. $\square$

Proposition 3.2.58. *Let $V = F^m$ be a regular near-vector over a finite field of order q. Then $\Gamma_{\mathcal{I}}(V)$ is a graph of order*

$$\sum_{t=1}^{m-1} \binom{m}{t}_q.$$

Proof. Since the number of t-dimensional subspaces of an m-dimensional near-vector space over a finite field of order q is the q-binomial coefficient

$$\binom{m}{t}_q = \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-t+1}-1)}{(q^t-q)(q^{t-1}-1)\cdots q-1)},$$

the total number of nontrivial proper subspaces of V is given by

$$\sum_{t=1}^{m-1} \binom{m}{t}_q.$$

□

Finally, we look at the degree of a proper non-trivial subspace of V.

Theorem 3.2.59. *If W is a t-dimensional non-trivial proper subspace of a regular near-vector space V defined over $F = GF(q)$, then $\deg(W)$ in $\Gamma_{\mathcal{I}}(V)$ is*

$$\sum_{i=1}^{t-1} \binom{t}{i}_q + \sum_{i=1}^{m-t-1} \binom{m-t}{i}_q.$$

Proof. The proof is divided into the case where we count the number of t-dimensional distinct non-trivial proper subspaces that are contained in W, and the case where we count the number of t-dimensional distinct non-trivial proper subspaces that contain W. For the first case, we have

$$\sum_{i=1}^{t-1} \binom{t}{i}_q$$

number of t-dimensional non-trivial proper subspaces contained in W. In the second case, we observe that the number of non-trivial proper subspaces strictly between W and V are exactly the number of subspaces strictly contained in the regular quotient space V/W (see Proposition 3.3.11). The dimension of V/W is $m-t$, and therefore, for the second case we have

$$\sum_{i=1}^{m-t-1} \binom{m-t}{i}_q$$

number of t-dimensional non-trivial proper subspaces containing W, and the result follows.

□

For non-regular near-vector spaces, the above formulae need to be amended. Suppose $V = V_1 \oplus \cdots \oplus V_k$ is the canonical decomposition of a non-regular near-vector space over a finite field $F = GF(q)$. The degree of a t-dimensional non-trivial proper subspace W will be determined for each of the regular maximal subspaces V_i of V, where $i \in \{1, \ldots, k\}$. Additionally, we need to compensate for each of the V_i, for $i \in \{1, \ldots, k\}$, being a subspace of V.

Corollary 3.2.60. *Let (V, F) be a non-regular near-vector space defined as above, where*

$$V = V_1 \oplus \cdots \oplus V_k$$

is the canonical decomposition of V. Then

$$deg(W_i) = \begin{cases} \sum_{j=1}^{t-1} \begin{bmatrix} t \\ j \end{bmatrix}_q + \sum_{j=1}^{m_i - t - 1} \begin{bmatrix} m_i - t \\ j \end{bmatrix}_q + 1 & , \quad \text{if } dim(V_i) = m_i > t \\ \sum_{j=1}^{t-1} \begin{bmatrix} t \\ j \end{bmatrix}_q + \sum_{j=1}^{m_i - t - 1} \begin{bmatrix} m_i - t \\ j \end{bmatrix}_q & , \quad \text{if } dim(V_i) = m_i = t \end{cases}$$

in $\Gamma_{\mathcal{I}}(V)$, where W_i denotes a t-dimensional regular subspace of V and $t \leq m_i$, for $i \in \{1, \ldots, k\}$.

Proof. The proof follows from Theorem 3.2.59 and the fact that we have to compensate for the maximal regular subspace V_i, for each $i \in \{1, \ldots, k\}$. □

Consider the following example:

Example 3.2.61. *Referring to Example 3.2.55, let $V = F^5$ over finite field $F = \mathbb{Z}_5$, defined for all $(x_1, x_2, x_3, x_4, x_5) \in V$ and $\alpha \in F$ by*

$$(x_1, x_2, x_3, x_4, x_5)\alpha = (x_1\alpha^3, x_2\alpha^3, x_3\alpha^3, x_4\alpha, x_5\alpha).$$

The subspace inclusion graph of V has 2 components consisting of a 3-partite and 2-partite graph, respectively.

If we want to find the degree of the 2-dimensional subspaces, deg(W_i), then

$$\deg(W_i) = \begin{cases} \sum_{j=1}^{1} \binom{2}{j}_5 + 1 \quad , & \text{if } dim(V_1) > 2 \\ \sum_{j=1}^{1} \binom{2}{j}_5 \quad , & \text{if } dim(V_2) = 2 \end{cases}$$

$$= \begin{cases} \binom{2}{1}_5 + 1 \quad , & \text{if } dim(V_1) > 2 \\ \binom{2}{1}_5 \quad , & \text{if } dim(V_2) = 2 \end{cases}$$

$$= \begin{cases} 7 \quad , & \text{if } dim(V_1) > 2 \\ 6 \quad , & \text{if } dim(V_2) = 2 \end{cases}$$

Proposition 3.2.62. *Let (V, F) be a non-regular near-vector space defined over $F = GF(q)$ and let $V = V_1 \oplus \cdots \oplus V_k$ be the canonical decomposition of V. For $i \in \{1, \ldots, k\}$, if $\dim V_i = s_i$, then the subspace inclusion graph $\Gamma_{\mathcal{I}}(V)$ consists of k components of s_i-partite graphs, respectively.*

Proof. By Theorem 3.2.56, each component V_i of the canonical decomposition of V has an s_i-partite graph associated with it, for $i \in \{1, \ldots, k\}$. Therefore the result holds. □

In the proof of Theorem 3.2.59 we touched on the concept of the quotient space V/W. In the next section, we study this space more closely.

3.3 Some constructions of near-vector spaces

The work presented in Theorem 3.3.1 to Proposition 3.3.7 is based on unpublished results by K-T. Howell and C. Kestner. As a result we include the proofs of the results.

3.3.1 Direct sums of near-vector spaces

In this section we focus on the direct sum of subspaces of a given near-vector space.

The following theorem is not difficult to prove. We use it to define the direct sum of two subspaces.

Theorem 3.3.1. *Let (V, A) be a near-vector space and W_1 and W_2 be subspaces of V. Then the following conditions are equivalent:*

(i) $W_1 \cap W_2 = \{0\}$.

(ii) Every vector x in $W_1+W_2 := \{w_1+w_2 \mid w_1 \in W_1, w_2 \in W_2\}$ is uniquely representable in the form $x = w_1 + w_2$, with $w_1 \in W_1$ and $w_2 \in W_2$.

Definition 3.3.2. *If (V, A) is a near-vector space which satisfies the conditions of Theorem 3.3.1, then W_1+W_2 is called the direct sum of W_1 and W_2 and is denoted by $W_1 \oplus W_2$.*

The following theorem proved by Howell, exhibits a basis for $V = W_1 \oplus W_2$ in terms of bases of the complementary subspaces W_1 and W_2.

Theorem 3.3.3. *Let (V, A) be a near-vector space and W_1 and W_2 finite-dimensional subspaces of V such that $V = W_1 \oplus W_2$. Then V is a finite-dimensional near-vector space. Moreover, if $\mathcal{B} = \{x_1, x_2 \ldots, x_k\}$ is a basis for W_1 and $\mathcal{C} = \{y_1, y_2, \ldots, y_m\}$ a basis for W_2, then $\mathcal{K} = \{x_1, x_2, \ldots, x_k, y_1, y_2 \ldots, y_m\}$ is a basis for V. Thus $\dim V = \dim W_1 + \dim W_2$.*

Proof. To show that $\mathcal{K} \subseteq Q(V)$, we have by Lemma 2.2.8 that $Q(W_i) \subseteq Q(V)$ for $i \in \{1, 2\}$. Since $\mathcal{B} \subseteq Q(W_1)$ and $\mathcal{C} \subseteq Q(W_2)$, we have that both $\mathcal{B}$ and $\mathcal{C}$ are contained in $Q(V)$. Hence $\mathcal{K} \subseteq Q(V)$.
For each $v \in Q(V)$, by Theorem 3.3.1(ii) we can write $v = w_1 + w_2$ for some $w_1 \in W_1$ and $w_2 \in W_2$. Then for some $\alpha_i, \beta_j \in A$, $x_i \in \mathcal{B}, y_j \in \mathcal{C}$,

$$\begin{aligned} v &= w_1 + w_2 \\ &= \sum_{i=1}^{k} x_i\alpha_i + \sum_{j=1}^{m} y_j\beta_j, \end{aligned}$$

since $\mathcal{B}$ and $\mathcal{C}$ are bases for W_1 and W_2, respectively. Therefore, $\mathcal{K}$ generates $Q(V)$. Since $W_1 \cap W_2 = \{0\}$, it is easy to show that the vectors in $\mathcal{K}$ are linearly independent. □

The following proposition generalises the idea of the direct sum of subspaces of a near-vector space.

Proposition 3.3.4. *Let (V, A) be a near-vector space and $W_1, W_2, \ldots, W_n$ be subspaces of V. Then the following conditions are equivalent:*
(i) $W_i \cap W_j = \{0\}$ whenever $i \neq j$;
(ii) Every vector x in $W_1 + W_2 + \cdots + W_n$ is uniquely representable in the form $x = w_1 + w_2 + \ldots + w_n$, with $w_i \in W_i$ for $i \in \{1, \ldots, n\}$.

Remark 3.3.5.
Just as the idea of the direct sum of two subspaces of a near-vector space in Proposition 3.3.1 is generalised in the above proposition, similarly Theorem 3.3.3 can also be generalised to a direct sum of a finite number of subspaces.

3.3.2 Quotients of near-vector spaces

In this section, we explore the quotient subspaces of a near-vector space. Although the work done by Howell and Kestner constructed the near-vector spaces over A, our work will focus mainly on finite-dimensional near-vector spaces over finite fields.

We start by proving that addition and scalar multiplication in the quotient space is well-defined.

Proposition 3.3.6. *Let W be a subspace of a near-vector space (V, A), then for all $v_1, v_2 \in V$ and $\alpha \in A$ the following operations:*

(i) $(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$;
(ii) $(v_1 + W)\alpha = v_1\alpha + W$,

are well defined on the set $V/W = \{v + W | v \in V\}$.

Proof. Suppose for all $v_1, v_2, v_1', v_2' \in V$ and $\alpha \in A$ we have that $v_1 + W = v_1' + W$ and $v_2 + W = v_2' + W$, then this implies that $v_i - v_i' \in W$ for $i \in \{1, 2\}$. Thus there exists some $w_1, w_2 \in W$ such that $v_i - v_i' = w_i$ for $i \in \{1, 2\}$. It follows that $v_i = v_i' + w_i$ for $i \in \{1, 2\}$, then

$$\begin{aligned}(v_1 + W) + (v_2 + W) &= (v_1 + v_2) + W \\ &= ((v_1' + w_1) + (v_2' + w_2)) + W \\ &= (v_1' + v_2') + (w_1 + w_2) + W \\ &= (v_1' + v_2') + W \quad \text{since } w_1, w_2 \in W,\ w_1 + w_2 \in W \\ &= (v_1' + W) + (v_2' + W)\end{aligned}$$

and

$$\begin{aligned}(v_1 + W)\alpha &= v_1\alpha + W \\ &= (v_1' + w_1)\alpha + W \\ &= v_1'\alpha + w_1\alpha + W \\ &= v_1'\alpha + W \quad \text{since } W \text{ is closed under scalar multiplication} \\ &= (v_1' + W)\alpha.\end{aligned}$$

□

In 2016, Kestner proved the following theorem. We include its proof for completeness. It may seem straightforward to show that if W is a subspace, V/W will be a near-vector space, but proving that A acts fixed point free on V/W and showing that $Q(V/W)$ generates V/W requires some work. In fact, we get that a subset of $Q(V/W)$ generates V/W.

Theorem 3.3.7. *Let W be a subspace of a near-vector space (V, A) and $V/W = \{v + W | v \in V\}$. Then V/W (as an abelian group) under the operations of Proposition 3.3.6 is a near-vector space over A, called the quotient near-vector space.*

Proof. Proposition 3.3.6 shows that the operations are well-defined. Next we verify the axioms of a near-vector space for $(V/W, A)$.

(a) $(V/W, A)$ is an abelian group:
It is clear that V/W with the induced addition is an abelian group.

(b) A acts as a set of endomorphisms on $(V/W, +)$:
For $\lambda \in A$ and $v_1 + W,\ v_2 + W \in V/W$, for $v_1, v_2 \in V$, we have

$$\begin{aligned}[(v_1 + W) + (v_2 + W)]\lambda &= ((v_1 + v_2) + W)\,\lambda \\ &= (v_1 + v_2)\lambda + W \\ &= (v_1\lambda + v_2\lambda) + W \\ &= (v_1\lambda + W) + (v_2\lambda + W) \\ &= (v_1 + W)\lambda + (v_2 + W)\lambda.\end{aligned}$$

Also,

(i) $(v_1 + W)0 = (v_1)0 + W = 0 + W = W$;

(ii) $(v_1 + W)1 = (v_1)1 + W = v_1 + W$; and

(iii) $(v_1 + W)(-1) = (v_1)(-1) + W = (-v_1) + W$.

(c) $(A^*, \circ)$ is a subgroup of $(\mathrm{Aut}(V/W), \circ)$ follows from the fact that $(A^*, \circ)$ is a subgroup of $(Aut(V), \circ)$.

(d) We need to show that A acts fixed point free on V/W. Let X be a subset of $Q(V)$ such that XA generates W. We want to show that for $v + W \in V/W$ and $\alpha, \beta \in A$,

$$(v + W)\alpha = (v + W)\beta,$$

implies that $\alpha = \beta$ or $v + W = 0 + W$.
We start by showing that $\langle Q(V) \setminus XA^* \rangle$ is closed under the action of A. Suppose $v \in \langle Q(V) \setminus XA^* \rangle$, then for $b_1, ..., b_n \in Q(V) \setminus XA^*$ we have that

$$v = \sum_{i=1}^{n} b_i\alpha_i,$$

where $\alpha_i \in A$. If $\alpha \in A$, then

$$\begin{aligned} v\alpha &= \sum_{i=1}^{n} (b_i\alpha_i)\alpha \\ &= \sum_{i=1}^{n} b_i(\alpha_i\alpha). \end{aligned}$$

Then $\alpha_i\alpha \in A$ since A^* is a subgroup of the automorphism group. Therefore, $b_i(\alpha_i\alpha) \in Q(V) \setminus XA^*$. By definition $\langle Q(V) \setminus XA^* \rangle$ is closed under addition of vectors, hence $v\alpha \in \langle Q(V) \setminus XA^* \rangle$.

Now suppose we have $v + W \in (V/W) \setminus \{0 + W\}$ and $\alpha, \beta \in A$ such that

$$\begin{aligned} &(v + W)\alpha = (v + W)\beta \\ \implies\ &v\alpha + W = v\beta + W. \end{aligned}$$

This implies that $v\alpha - v\beta \in W$. We may assume that $v \in \langle Q(V) \setminus XA^* \rangle$ since we assumed that $v \notin W$. So $v\alpha, v\beta \in \langle Q(V) \setminus XA^* \rangle$ and therefore

$$v\alpha - v\beta \in \langle Q(V) \setminus XA^* \rangle.$$

This implies that

$$v\alpha - v\beta \in \langle Q(V) \setminus XA^* \rangle \cap W.$$

Note that $\langle Q(V) \setminus XA^* \rangle \cap W = \{0\}$ since $\langle Q(V) \setminus XA^* \rangle = Q(V) \setminus W \cup \{0\}$. So in V, $v\alpha - v\beta = 0$ and by the fixed point free property of A on V we have that $\alpha = \beta$ or $v = 0$. Since $v \notin W$ we have that $v + W \neq 0 + W$, and

$$v\alpha + W = v\beta + W$$

implies that $\alpha = \beta$.

(e) We will show that $Q(V)/W$ generates V/W. We begin by showing that $Q(V)/W \subseteq Q(V/W)$. Let $a + W \in Q(V)/W$ for $a \in Q(V)$. Then for all $\alpha, \beta \in A$, there exists a $\gamma \in A$ such that $a\alpha + a\beta = a\gamma$. Thus

$$\begin{aligned} (a + W)\alpha + (a + W)\beta &= (a\alpha + a\beta) + W \\ &= a\gamma + W \\ &= (a + W)\gamma. \end{aligned}$$

Thus $a + W \in Q(V/W)$. If $Q(V)$ generates V, then $Q(V)/W$ will generate V/W. Furthermore, since we have shown that $Q(V)/W \subseteq Q(V/W)$, we have that $Q(V/W)$ generates V/W.

□

Kestner showed in the above theorem that $Q(V)/W \subseteq Q(V/W)$. A natural question to ask is under what conditions will $Q(V/W)$ ever be equal to $Q(V)/W$? We will answer this question later in the thesis. But first, we address the issue of using different coset representatives and whether this has any impact on the γ which is uniquely determined, according to the definition of the quasi-kernel.

Lemma 3.3.8. *Let (V, A) be a near-vector space, W a subspace of V and $a+W, a'+W \in (Q(V)/W)^*$. If $a+W = a'+W$, then for all $\alpha, \beta \in A$,*

$$\alpha +_{a+W} \beta = \alpha +_{a'+W} \beta.$$

Proof. Since $a + W \in (Q(V)/W)^*$, there exists a γ for all $\alpha, \beta \in A$ such that

$$(a+W)(\alpha +_{a+W} \beta) = (a+W)\alpha + (a+W)\beta = (a+W)\gamma.$$

We need to show that γ is independent of the choice of coset representative. So, suppose

$$\begin{aligned} & a' + W = a + W, \\ \implies\ & a' - a \in W. \end{aligned}$$

Let $w = a' - a$ for some $w \in W$, or $a' = w + a$. Then

$$\begin{aligned} (a'+W)\alpha + (a'+W)\beta &= (w+a+W)\alpha + (w+a+W)\beta \\ &= (a+W)\alpha + (a+W)\beta, \quad \text{since } w \in W \text{ and } V \text{ abelian} \\ &= (a+W)\gamma \\ &= (a'+W)\gamma. \end{aligned}$$

Therefore,

$$\alpha +_{a+W} \beta = \gamma = \alpha +_{a'+W} \beta.$$

□

We can now construct a basis for $(V/W, A)$:

Theorem 3.3.9. *Let (V, A) be a near-vector space and W a subspace of V. Suppose $\{w_1, \ldots, w_m\}$ and $\{w_1, \ldots, w_m, v_1, \ldots, v_n\}$ are bases of W and V, respectively. Then*

$$\mathcal{B} = \{v_1 + W, \ldots, v_n + W\}$$

is a basis of V/W, i.e. $\dim V/W = \dim V - \dim W$.

Proof. $\mathcal{B} \subseteq Q(V/W)$ by Theorem 3.3.7 (e), since $\{v_1, \ldots, v_n\} \subseteq Q(V)$. Next we show that $\mathcal{B}$ generates $Q(V/W)$. Let $x \in Q(V/W)$, then $x = v + W$ for some $v \in V$. But we can also write v as follows:

$$v = \sum_{j=1}^{m} w_j \eta_j + \sum_{i=1}^{n} v_i \varepsilon_i,$$

where $\eta_j, \varepsilon_i \in A$ for $j \in J := \{1, \ldots, m\}$ and $i \in I := \{1, \ldots, n\}$. Therefore,

$$\begin{aligned} x &= v + W \\ &= \sum_{j=1}^{m} w_j \eta_j + \sum_{i=1}^{n} v_i \varepsilon_i + W \\ &= \sum_{i=1}^{n} v_i \varepsilon_i + W \\ &= \sum_{i=1}^{n} (v_i + W) \varepsilon_i, \end{aligned}$$

since $\sum_{j=1}^{m} w_j \eta_j \in W$ and V is abelian. Finally, we need to show that $\mathcal{B}$ is linearly independent. Suppose $\sum v_i \alpha_i + W = 0 + W = W$, which implies that $\sum v_i \alpha_i \in W$. Then for some $\eta_j \in A$ we have that

$$\begin{aligned} \sum v_i \alpha_i &= \sum w_i \eta_j \\ \sum v_i \alpha_i + \sum w_i (-\eta_j) &= 0. \end{aligned}$$

But $\{w_1, \ldots, w_m, v_1, \ldots, v_n\}$ is linearly independent, so $\alpha_i = \eta_j = 0$ for all $i \in I$, $j \in J$, by Proposition 2.2.3. □

To prove our main results we return to the block constructions of Section 2.2, i.e. $V = F^m$ is a near-vector space defined over finite field $F = GF(p^r)$, for some p a prime and $r \in \mathbb{N}$. For $\alpha \in F$ and $(x_1, \ldots, x_m) \in V$ define scalar multiplication by

$$(x_1, \ldots, x_m)\alpha = (x_1 \psi_1(\alpha), \ldots, x_m \psi_m(\alpha)),$$

where the $\psi_i : (F, \cdot) \to (F, \cdot)$ are multiplicative semi-group automorphisms for $i \in \{1, \ldots, m\}$. For $I = \{1, \ldots, m\}$, let $A_j = \{i \in I | \psi_i(\alpha) = \psi_j(\alpha^{p^l}) \text{ for some } l \in \{0, \ldots, r-1\}\}$, then the A_j, for $j \in \{1, \ldots, k\}$, give a partition of I. If V is not regular, then we can canonically decompose it as $V = V_1 \oplus \cdots \oplus V_k$ where the V_i, $i \in \{1, \ldots, k\}$ is a maximal regular subspace of V. Suppose the dimension of V_i, $\dim V_i = m_i$, for $i \in \{1, 2 \ldots, k\}$. From now on let $K := \{1, 2, \ldots, k\}$.

To illustrate the next result, we begin with a simple example.

Example 3.3.10.
Let $V = F^3$ where $F = \mathbb{Z}_5$ and suppose for all $(x, y, z) \in V$ and $\alpha \in F$ scalar multiplication is defined by

$$(x, y, z)\alpha = (x\alpha^3, y\alpha^3, z\alpha^3).$$

Then (V, F) is a regular near-vector space. Since F is a finite field by Theorem 2.2.46, we have that $Q(V) = V$ if and only if V is regular. Now, consider the subspace W of V, where

$$W = \{(a, 0, c) \mid a, c \in F\}.$$

By Lemma 2.2.17, W is regular and thus $Q(W) = W$ by Theorem 2.2.46. The quotient space V/W will be given by

$$\begin{aligned} V/W &= \{(x, y, z) + W \mid (x, y, z) \in V\} \\ &= \{(0, y, 0) + W \mid y \in F\}. \end{aligned}$$

Let $(0, y, 0) + W \in V/W$ and $\alpha, \beta \in F$, then

$$\begin{aligned} ((0, y, 0) + W)\alpha + ((0, y, 0) + W)\beta &= (0, y, 0)\alpha + W + (0, y, 0)\beta + W \\ &= (0, y\alpha^3, 0) + (0, y\beta^3, 0) + W \\ &= (0, y\alpha^3 + y\beta^3, 0) + W \\ &= (0, y(\alpha^3 + \beta^3), 0) + W \\ &= (0, y, 0)(\alpha^3 + \beta^3)^{\frac{1}{3}} + W, \end{aligned}$$

where $\gamma = (\alpha^3 + \beta^3)^{\frac{1}{3}} \in F$, a well-known result. (See [1], for example). Thus $V/W \subseteq Q(V/W)$ and so $V/W = Q(V/W)$. Thus $(V/W, A)$ is regular. ◊

This leads us to:

Proposition 3.3.11. *Let (V, F) be a near-vector space where F is a finite field and W a subspace of V. If V is regular, then V/W is regular.*

Proof. We need to show that $Q(V/W) = V/W$. Since we have that $Q(V/W) \subseteq V/W$, we show the other inclusion. Let $v + W \in V/W$, where $v \notin W$. Since V is regular, we have that $Q(V) = V$, and so $v \in Q(V)$. By Theorem 3.3.7 (e) we have that $v + W \in Q(V/W)$. This implies $V/W \subseteq Q(V/W)$ and hence $Q(V/W) = V/W$. □

The converse of Proposition 3.3.11 is not true, in general, that is, V/W being regular does not imply that V is regular. The next example illustrates this point.

Example 3.3.12.
Consider the near-vector space $V = F^4$, where $F = \mathbb{Z}_{11}$. Suppose scalar multiplication is

defined for all $(x_1, x_2x_3, x_4) \in V$ *and* $\alpha \in F$ *by:*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha^5, x_4\alpha^3).$$

Then

$$Q(V) = \{(a, 0, 0, 0)|a \in F\} \cup \{(0, b, 0, d)|b, d \in F\} \cup \{(0, 0, c, 0)|c \in F\}.$$

For $(1, 0, 0, 0)$ *and* $(0, 0, 1, 0) \in Q(V)$ *and for all* $\lambda \in F^*$,

$$(1, 0, 0, 0) + (0, 0, 1, 0)\lambda = (1, 0, \lambda^5, 0) \notin Q(V).$$

Hence, V *is not regular. We have that* V *decomposes as:*

$$\begin{aligned} V &= V_1 \oplus V_2 \oplus V_3 \\ &= \{(a, 0, 0, 0)|a \in F\} \oplus \{(0, b, 0, d)|b, d \in F\} \oplus \{(0, 0, c, 0)|c \in F\}. \end{aligned}$$

Now consider $V/(V_1 \oplus V_2)$ *where* $V_1 = \{(a, 0, 0, 0)|a \in F\}$ *and* $V_2 = \{(0, b, 0, d)|b, d \in F\}$. *Then*

$$\begin{aligned} V/(V_1 \oplus V_2) &= \{(a, b, c, d) + (V_1 \oplus V_2)|a, b, c, d \in F\} \\ &= \{(a, 0, 0, 0) + (0, b, 0, d) + (0, 0, c, 0) + (V_1 \oplus V_2)|a, b, c, d \in F\} \\ &= \{(0, 0, c, 0) + (V_1 \oplus V_2)|c \in F\}. \end{aligned}$$

We claim that $V/(V_1 \oplus V_2)$ *is regular. Let* $\alpha, \beta \in F$ *and* $(0, 0, c, 0) + (V_1 \oplus V_2) \in V/(V_1 \oplus V_2)$ *for* $c \in F$. *Then*

$$\begin{aligned} ((0, 0, c, 0) + (V_1 \oplus V_2))\,\alpha + ((0, 0, c, 0) + (V_1 \oplus V_2))\,\beta &= (0, 0, c\alpha^5 + c\beta^5, 0) + (V_1 \oplus V_2) \\ &= (0, 0, c(\alpha^5 + \beta^5), 0) + (V_1 \oplus V_2) \\ &= ((0, 0, c, 0) + (V_1 \oplus V_2))\,(\alpha^5 + \beta^5)^{\frac{1}{5}}, \end{aligned}$$

where $\gamma = (\alpha^5 + \beta^5)^{\frac{1}{5}} \in F$ *(see [1], for example). We have that* $(0, 0, c, 0) + (V_1 \oplus V_2) \in Q(V/(V_1 \oplus V_2))$, *so* $V/(V_1 \oplus V_2) \subseteq Q(V/(V_1 \oplus V_2))$. *Now since* $Q(V/(V_1 \oplus V_2)) \subseteq V/(V_1 \oplus V_2)$, *we have that* $Q(V/(V_1 \oplus V_2)) = V/(V_1 \oplus V_2)$. *Thus* $V/(V_1 \oplus V_2)$ *is regular.* ◊

We will need the following result.

Proposition 3.3.13. *Suppose* (V, F) *is a non-regular near-vector space with canonical decomposition* $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$. *If* $W = \bigoplus_{j \in J} V_j$, *where* $J \subset K$, $Q(W) = \bigcup_{j \in J} V_j$ *and* W *is a subspace of* V.

Proof. W is a subset of V generated by $Q(W) = \bigcup_{j \in J} V_j \subset Q(V)$. □

Next, we look at what happens if (V, F) is non-regular and we take W to be the direct sum of some but not all of the maximal regular subspaces V_i, $i \in \{1, \ldots, k\}$ where the V_i's are not necessarily consecutive to one another.

By Theorem 3.3.7, $Q(V)/W \subseteq Q(V/W)$ where V/W is a near-vector space over A. However, if A is a finite field, then under certain conditions $Q(V)/W = Q(V/W)$.

Lemma 3.3.14. *Let (V, F) be a non-regular near-vector space over a finite field $F = GF(p^r)$, where $V = F^m$. Let $V = V_1 \oplus \cdots \oplus V_k$ be the canonical decomposition of V and we take the direct sum of $W = \bigoplus_{j \in J} V_j$, for $J \subseteq K$ and $|J| \leq |K| - 1$. Then $Q(V/W) = Q(V)/W$.*

Proof. By Theorem 3.3.7 (e) we have that $Q(V)/W \subseteq Q(V/W)$. Conversely, let $v' + W \in Q(V/W)$, where $v' + W \neq W$. Then for all $\alpha,\ \beta \in F$ there exists an $\gamma \in F$ such that

$$\begin{aligned}(v' + W)\alpha + (v' + W)\beta &= (v' + W)\gamma \\ \implies (v'\alpha + v'\beta) + W &= v'\gamma + W.\end{aligned}$$

This implies that $v'\alpha + v'\beta - v'\gamma \in W$. On the other hand, we have

$$\begin{aligned}Q(V)/W &= (V_1 \cup \cdots \cup V_k)/W \\ &= (\bigcup_{s \notin J} V_s + W)/W.\end{aligned}$$

Then

$$v' \in \bigoplus_{s \in K \setminus J} V_s$$

and by Theorem 3.3.3 and Remark 3.3.5, $\bigoplus_{s \in K \setminus J} V_s$ is a near-vector space. Thus,

$$v'\alpha + v'\beta - v'\gamma \in \bigoplus_{s \in K \setminus J} V_s.$$

We also have that $v'\alpha + v'\beta - v'\gamma \in W$ and $\bigoplus_{s \in K \setminus J} V_s \cap W = \{0\}$, so

$$\begin{aligned}v'\alpha + v'\beta - v'\gamma &= 0 \\ v'\alpha + v'\beta &= v'\gamma\end{aligned}$$

This means that v' is ultimately in $Q(V)$, which implies that $v' + W \in Q(V)/W$ and we have that $Q(V/W) \subseteq Q(V)/W$. Hence, $Q(V/W) = Q(V)/W$. □

Moreover, it becomes clear that what is factored out plays a role in the regularity of the quotient space.

Example 3.3.15.
Consider the near-vector space in Example 3.3.12, where $V = F^4$, $F = \mathbb{Z}_{11}$, and scalar multiplication is defined as above.

Let us consider

$$\begin{aligned} V/V_3 &= \{(a,b,c,d) + V_3 | a,b,c,d \in F\} \\ &= \{(a,b,0,d) + V_3 | a,b,d \in F\}. \end{aligned}$$

We claim that V/V_3 is not regular. Since V_3 is regular, by Theorem 2.2.46 $Q(V_3) = V_3$ and we have that

$$\begin{aligned} Q(V/V_3) &= Q(V)/Q(V_3) \text{ by Lemma 3.3.14} \\ &= Q(V)/V_3 \\ &= \{(a,b,c,d) + V_3 | (a,b,c,d) \in Q(V)\} \\ &= \{(a,0,0,0) + V_3 | a \in F\} \cup \{(0,b,0,d) + V_3 | b,d \in F\} \cup \{V_3\} \\ &= \{(a,0,0,0) + V_3 | a \in F\} \cup \{(0,b,0,d) + V_3 | b,d \in F\}, \end{aligned}$$

since V_3 is contained in each of the sets in the union. If we take $(1,0,0,0) + V_3$ and $(0,1,0,1) + V_3$, then for any $\lambda \in F^*$,

$$\begin{aligned} ((1,0,0,0) + V_3) + ((0,1,0,1) + V_3)\lambda &= ((1,0,0,0) + (0,1,0,1)\lambda) + V_3 \\ &= (1, \lambda^3, 0, \lambda^3) + V_3 \notin Q(V/V_3). \end{aligned}$$

Thus V/V_3 is not regular. ◊

As stated before, we have that $Q(V) = V$ if and only if V is regular for any near-vector space V defined over a finite field F. The next theorem proves an analogous result for the near-vector space V/W defined over a finite field F, in the special case where the subspace W is defined as the sum of some of the maximal regular subspaces of V.

Theorem 3.3.16. *Let (V, F) be a non-regular near-vector space over a finite field $F = GF(p^r)$, where $V = F^m$ and the scalar multiplication is defined for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$ by*

$$(x_1, \ldots x_m)\alpha = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)),$$

where the ψ_i's are automorphisms of $(F, \cdot)$ for $i \in I$. Let $V = V_1 \oplus \cdots \oplus V_k$ be the canonical decomposition of V and $W = \bigoplus_{j \in J} V_j$, for $J \subset K$. Then the following are equivalent:

1. *V/W is regular;*
2. *$V/W = (V_i + W)/W$ for some $i \in K \setminus J$;*

3. $Q(V/W) = V/W$.

Proof. Let $W' = \bigoplus_{j \in K \setminus J} V_j$. By Proposition 3.3.13, W' is a subspace of V. Define a mapping $\theta : W' \to V/W$ by $\theta(v) = v + W$. Next let $\eta : (F, \cdot) \to (F, \cdot)$ be the identity mapping. Then it is not difficult to check that (θ, η) is a near-vector space isomorphism.

1 $\implies$ 2: Suppose that V/W is regular. Then W' must be regular by Theorem 2.2.22. Thus $W' \subseteq V_i$ for some $i \in K \setminus J$, but W is the direct some of all the subspaces V_j with $j \in K \setminus J$, so $V_i \subseteq W'$, so $V_i = W'$. This gives that $V/W = (V_i + W)/W$ for some $i \in K \setminus J$.

2 $\implies$ 3: Suppose that $V/W = (V_i + W)/W$ for some $i \in K \setminus J$. We already have that $Q(V/W) \subseteq V/W$. Now let $v + W \in V/W$, then $v \in V_i = Q(V_i)$, for some $i \in K$ so that $v \in Q(V)$. Thus $V/W \subseteq Q(V/W)$ and thus $Q(V/W) = V/W$.

3 $\implies$ 1: Suppose that $Q(V/W) = V/W$. By Theorem 2.2.25, $\theta(Q(W')) = Q(V/W) = V/W$. Thus we get that $\theta(Q(W')) = (W' + W)/W$, so that by Theorem 2.2.25 , W' is regular, giving by Theorem 2.2.46 that V/W is regular. □

We begin by determining the cardinality of V/W' where we quotient out by all but one maximal regular subspace.

Theorem 3.3.17. *Let (V, F) be a non-regular near-vector space over a finite field $F = GF(p^r)$, where $V = F^m$. Let $V = V_1 \oplus \cdots \oplus V_k$ be the canonical decomposition of V and $W = \bigoplus_{j \in J} V_j$, for $J \subset K$ and $|J| = |K| - 1$. Then we have that*

$$|Q(V/W)| = |Q(V_i)|,$$

for $i \in K \setminus J$.

Proof. By Lemma 3.3.14, $Q(V/W) = Q(V)/W$, thus $|Q(V/W)| = |Q(V_i)|$ since $V_i \cap W = \{0\}$. □

As we have found the cardinality of $Q(V/W)$, we can now define the regularity graph for the regular quotient space V/W.

Proposition 3.3.18. *Let (V, F) be a non-regular near-vector space over a finite field $F = GF(p^r)$, where $V = F^m$. Let $V = V_1 \oplus \cdots \oplus V_k$ be the canonical decomposition of V and $W = \bigoplus_{j \in J} V_j$, for $J \subset K$ and $|J| = |K| - 1$. Then $V/W = (V_i + W)/W$ for some $i \in K \setminus J$. The regularity graph Γ of the quotient space V/W is given by*

$$\Gamma(V/W) = K_{|Q(V_i)^*|}.$$

For our construction of V/W above, the cardinality of the pseudo-projective space, denoted $|P(V/W)|$, is given by $\frac{p^{r|A_i|-1}}{p^r-1}$, where $V/W = (V_i+W)/W$ and A_i is the cell in the partition of $\{1,2,\ldots,m\}$ corresponding to V_i, $i \in \{1,\ldots,k\}$. We now give the fibration graph of the near-vector space V/W.

Proposition 3.3.19. *Let (V,F) be a non-regular near-vector space over a finite field $F = GF(p^r)$, where $V = F^m$. Let $V = V_1 \oplus \cdots \oplus V_k$ be the canonical decomposition of V and $W = \bigoplus_{j\in J} V_j$, for $J \subset K$ and $|J| = |K| - 1$. Then $V/W = (V_i + W)/W$ for some $i \in K \setminus J$. The fibration graph $\Gamma_{\mathcal{F}}$ of the quotient space V/W is given by*

$$\Gamma_{\mathcal{F}}(V/W) = \bigcup_{j=1}^{|P(V_i)|} K_{|F^*|}.$$

We have encountered a case where the quotient space is not regular. A natural question is what can we say about the canonical decomposition of the space. Suppose V is not regular and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ is the canonical decomposition of V and let $W' = V_1 \oplus V_2 \oplus \cdots \oplus V_t$, where $t < k-1$. Then W' is a subspace of V and $Q(W') = V_1 \cup \cdots \cup V_t$ by Proposition 3.3.13. By Theorem 3.3.16, V/W' is not regular since $Q(V/W') \neq V/W'$ and we can show that:

Lemma 3.3.20. *Suppose (V,F) is a near-vector space, where $V = F^m$ and F is a finite field. Suppose V is not regular and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ is the canonical decomposition of V. Let $W' = V_1 \oplus V_2 \oplus \cdots \oplus V_t$, where $t < |K| - 1$. Then*

$$Q(V/W') = \bigcup_{i=t+1}^{k} (V_i + W')/W'.$$

Proof. We have that,

$$\begin{aligned} Q(V/W') &= Q(V)/W' \text{ by Lemma 3.3.14} \\ &= \{v + W' | v \in V_1 \cup \cdots \cup V_k\} \text{ by Lemma 2.2.44} \\ &= \{v + W' | v \in V_{t+1} \cup \cdots \cup V_k\} \\ &= \bigcup_{i=t+1}^{k} (V_i + W')/W'. \end{aligned}$$

□

In the following proposition we state what the canonical decomposition of V/W' will be.

Proposition 3.3.21. *Suppose (V, F) is a near-vector space, where $V = F^m$ and F is a finite field. Suppose V is not regular and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ is the canonical decomposition of V. Let $W' = V_1 \oplus V_2 \oplus \cdots \oplus V_t$, where $t < |K| - 1$. Then*

$$V/W' = \bigoplus_{i=t+1}^{k} (V_i + W')/W'$$

is the canonical decomposition of V/W'.

Proof. To show that $V/W' = \bigoplus_{i=t+1}^{k} (V_i + W')/W'$ is the canonical decomposition of V/W', we need to show that each $(V_i + W')/W'$ is a maximal regular subspace. It is clear that for any $i \in \{t+1, \ldots, k\}$, $(V_i + W')/W'$ is a subspace of V/W' (see Corollary 2.2.12). Let $v + W' \in (V_i + W')/W'$, then for $\alpha, \beta \in F$ we have for

$$\begin{aligned}(v + W')\alpha + (v + W')\beta &= (v\alpha + v\beta) + W' \\ &= v\gamma + W' \\ &= (v + W')\gamma\end{aligned}$$

for $\gamma \in F$, since we have that $Q(V_i) = V_i$ for $i \in \{1, \ldots, k\}$. Therefore for each $i \in \{t + 1, \ldots k\}$, $(V_i + W')/W'$ is a regular subspace of V/W'. Furthermore, for each $i \in \{t + 1, \ldots k\}$, $(V_i + W')/W'$ are maximal, by definition of the block construction. □

The following example illustrates the canonical decomposition of a quotient space that is non-regular.

Example 3.3.22.
Refer back to Example 3.3.15, where $V = F^4$, $F = \mathbb{Z}_{11}$ and scalar multiplication is defined for all $(x_1, x_2, x_3, x_4) \in V$ and $\alpha \in F$ by

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha^5, x_4\alpha^3).$$

Then

$$\begin{aligned}V &= V_1 \oplus V_2 \oplus V_3 \\ &= \{(a, 0, 0, 0) | a \in F\} \oplus \{(0, b, 0, d) | a \in F\} \oplus \{(0, 0, c, 0) | a \in F\},\end{aligned}$$

where

$$V/V_3 = \{(a, b, 0, d) + V_3 | a, b, d \in F\}$$

is not regular. Then we have that V/V_3 can be canonically decomposed as

$$\begin{aligned}V/V_3 &= \{v + V_3 | v \in V_1\} \oplus \{v + V_3 | v \in V_2\} \\ &= \{(a, 0, 0, 0) + V_3 | a \in F\} \oplus \{(0, b, 0, d) + V_3 | b, d \in F\},\end{aligned}$$

where $V_1/V_3 = Q(V_1/V_3) = \{(a, 0, 0, 0) + V_3 | a \in F\}$ and $V_2/V_3 = Q(V_2/V_3) = \{(0, b, 0, d) + V_3 | b, d \in F\}$. ◊

As with the case where V/W was regular, we now look at the cardinality of $Q(V/W')$, where V/W' is non-regular.

Theorem 3.3.23. *Let (V, F) be a near-vector space, where $V = F^m$ and $F = GF(p^r)$. Suppose V is non-regular and $V = V_1 \oplus \cdots \oplus V_k$ is the canonical decomposition of V. Let $W' = V_1 \oplus \cdots \oplus V_t$, where $t < |K| - 1$. Then*

$$|Q(V/W')| = \sum_{i=t+1}^{k} |Q(V_i)^*| + 1.$$

Proof. Since $Q(V/W') = \bigcup_{i=t+1}^{k} (V_i + W')/W'$ and the V_i's all have only the zero-vector in common, the result follows immediately. □

We now define the regularity and the fibration graphs for a non-regular space V/W over a finite field.

Proposition 3.3.24. *Suppose (V, F) is a near-vector space, where $V = F^m$ and $F = GF(p^r)$. Suppose V is non-regular and $V = V_1 \oplus \cdots \oplus V_k$ is the canonical decomposition of V. Let $W' = V_1 \oplus \cdots \oplus V_t$, where $t < |K| - 1$. Then the regularity graph Γ of the quotient space V/W' is given by*

$$\Gamma(V/W') = \bigcup_{i=t+1}^{k} K_{|Q(V_i)^*|}.$$

Proposition 3.3.25. *Suppose (V, F) is a near-vector space, where $V = F^m$ and $F = GF(p^r)$. Suppose V is not regular and $V = V_1 \oplus \cdots \oplus V_k$ is the canonical decomposition of V. Let $W' = V_1 \oplus \cdots \oplus V_t$, where $t < |K| - 1$. Then the fibration graph $\Gamma_{\mathcal{F}}$ of the quotient space V/W' is given by*

$$\Gamma_{\mathcal{F}}(V/W') = \bigcup_{i=t+1}^{k} \Gamma_{\mathcal{F}_i}(V/W'),$$

where $\Gamma_{\mathcal{F}_i}(V/W') = \bigcup_{j=1}^{|P(V_i)|} K_{|F^*|}$.

In conclusion to this chapter, the quotient near-vector spaces over finite fields is the most significant part of this thesis. As such, we have investigated as many characteristics pertaining to the "normal" near-vector space over a finite field, ending with the regularity and fibration graphs.

Chapter 4

Some reconstruction problems for near-vector spaces

4.1 Introduction

The following is a classical type of problem in mathematics. If the structure S' is associated with each structure in S, does S' uniquely determine S? For example, in graph theory the reconstruction problem is an example of this type of problem. Here the focus is on reconstructing the graph using its subgraphs, obtained by deleting one vertex at a time.

We will focus on some reconstruction problems of the regularity and fibration graphs. If you are given a regularity graph, can you construct an associated near-vector space? This question was answered by S. Dorfling, K-T. Howell and S.P. Sanon in [12]. We discuss this in the first part of this section.

In the third and fourth part of this section, we investigate two reconstruction problems of near-vector spaces from fibrations and their graphs. And finally, we investigate reconstructing a finite Dickson near-field from a given graph with given order.

4.2 Reconstructing near-vector spaces from regularity graphs

The following reconstruction was done in [12], where a near-vector space (V, F) over F, where F is a finite field, is associated with a given regularity graph. Refer back to Definition 2.2.37, where a suitable sequence with respect to a finite field is defined.

Suppose we are given the regularity graph

$$\Gamma(V) = K_{\alpha_1} \cup K_{\alpha_2} \cup \cdots \cup K_{\alpha_k},$$

where $\alpha_i = p^{r_i} - 1$, $i = 1, \ldots, k$. We ask if it is possible to construct a near vector space, so that the regularity graph is that of the near-vector space.

We proceed with the following steps:

1. Let $V = (\mathrm{GF}(p^r))^m$ with $m = r_1 + r_2 + \ldots + r_k$ and $F = \mathrm{GF}(p^r)$.
2. Construct a partition $A_1, A_2, \ldots, A_k$ of m with $|A_i| = r_i$, where $i \in \{1, 2, \ldots, k\}$.
3. Next, construct a suitable sequence $(s_1, \ldots, s_k)$ where $s_1 \leq s_2 \leq \cdots \leq s_k$, for $i = 1, 2, \ldots, k$.
4. Define for all $(x_1, \ldots, x_m) \in V$ and $\alpha \in F$

$$(x_1, x_2, \ldots, x_m)\alpha = (x_1\alpha, x_2\alpha^{t_1}, \ldots, x_m\alpha^{t_{m-1}}),$$

   where $\alpha^{t_j} = \alpha^{s_i}$ for $j \in A_i$, $i = 1, 2, \ldots, k$ and $j \in \{1, 2, \ldots m-1\}$.
5. Then (V, F) is a near-vector space with regularity graph $\Gamma(V)$.

   If we chose a different partition of $\{1, 2, \ldots, m\}$, then we will get a different near-vector space, not necessarily isomorphic to the first. Conditions for when the near-vector spaces are isomorphic were given in Theorem 2.2.39.

To get a better understanding of the above algorithm, let us consider the following example.

Example 4.2.1.
Suppose we are given $\Gamma(V) = K_{3^3-1} \cup K_{3^6-1} \cup K_{3^3-1}$.

1. *Then* $r_1 = r_3 = 1$ *and* $r_2 = 2$ *and we have that* $m = 4$. *So* $V = (GF(3^3))^4$ *with* $F = GF(3^3)$.
2. $|A_1| = 1$, $|A_2| = 2$ *and* $|A_3| = 1$, *then* $A_1 = \{1\}$, $A_2 = \{3, 4\}$ *and* $A_3 = \{2\}$ *is a possible partition of* $\{1, 2, 3, 4\}$.
3. *The set of cosets determined by* $\langle 3 \rangle$ *in the group* $U(3^3 - 1)$ *is given by* $\{\{1, 3, 9\}$, $\{5, 15, 19\}$, $\{7, 11, 21\}$ $\{17, 23, 25\}\}$. *We can choose from the list of smallest members of each coset, that is* $\{1, 5, 7, 17\}$, *so that the third and the fourth entries of the suitable sequence coincide. So we can choose, for example, the sequence* $\{1, 5, 7, 7\}$.
4. *Then* (V, F) *a near-vector space of dimension 4, where the scalar multiplication is given for all* $(x_1, \ldots, x_m) \in V$ *and* $\alpha \in F$ *by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^5, x_3\alpha^7, x_4\alpha^7).$$

5. (V, F) *is a near-vector space with regularity graph* $\Gamma(V)$.

$\Diamond$

4.3 Reconstructing near-vector spaces from deleted fibres

We now return to fibrations, as discussed in Section 3.2.2. We ask the following question: if we are given all fibrations of a near-vector space with one fiber deleted from each, can we construct a near-vector space V over $\mathbb{Z}_p$, for p prime, such that $(V,+)$ is a fibered group for the fibration? We will use the material of Section 2.2.

Suppose that l fibrations are given. Put m equal to the tuple size of each fibre. Let $I=\{1,\ldots,\ m\}$. Then the following will provide a way for us to construct a fibered group from fibrations with deleted fibers.

1. Write down all the nonzero entries of the $\mathcal{F}_s$, $s\in\{1,\ldots,\ l\}$ without repetition, resulting in a set $\{v_1,\ldots,v_k\}$.
2. Find the first prime p such that $p>\max\{v_1,\ldots,\ v_k\}$. Put $F=\mathbb{Z}_p$ and $V=F^m$.
3. From each $\mathcal{F}_s$, $s\in\{1,\ldots,\ l\}$, select an $a_s\in V^*$ such that a_s has the maximum number of non-zero entries.
4. For $s\in\{1,\ldots,l\}$, consider a_s. Write down the positions in which the non-zero entries occur, put $A_s=\{j\in l|$ the jth entry of a_s is non-zero$\}$. These form the block partition of V.
5. For each $s\in\{1,\ldots,l\}$, choose a multiplicative automorphism, ψ_s of F^*.
6. Define for all $(x_1,\ldots,x_m)\in V$ and $\alpha\in F$,
$$(x_1,\ldots,x_m)\alpha=(x_1\psi_1(\alpha),\ldots,x_m\psi_m(\alpha)),$$
where $\psi_i=\psi_j$ if and only if $i,j\in A_s$.
7. Then (V,F) is a fibered group for the fibration. If we chose a different partition of $\{1,2,\ldots,m\}$, then we will get a different fibered group, not necessarily isomorphic to the first.

The following example illustrates the above algorithm.

Example 4.3.1.
Let
$$\mathcal{F}_i=\{aF|a\in V_i^*\},\quad i=1,2$$
where
$$\mathcal{F}_1=\{\{(1,0,0,0)F\},\{(1,0,1,0)F\},\{(2,0,1,0)F\},\{(1,0,4,0)F\},\{(3,0,1,0)F\}\}$$
and
$$\mathcal{F}_2=\{\{(0,1,0,1)F\},\{(0,2,0,0)F\},\{(0,0,0,3)F\},\{(0,1,0,2)F\},\{(0,1,0,3)F\}\}.$$

We know that the number of fibrations $l = 2$ and $m = 4$. If we follow the steps of the algorithm, then:

1. *The non-zero entries are $\{1, 2, 3, 4\}$.*
2. *The prime $p > \max\{1, 2, 3, 4\}$ is $p = 5$. Therefore $F = \mathbb{Z}_5$ and $V = F^4$.*
3. *$a_1 = (1, 0, 1, 0)$ and $a_2 = (0, 1, 0, 1)$.*
4. *$A_1 = \{1, 3\}$ and $A_2 = \{2, 4\}$.*
5. *For A_1 we choose the identity automorphism, and for A_2 the multiplicative automorphism, $\psi_2(\alpha) = \alpha^3$.*
6. *Define the scalar multiplication for all $(x_1, x_2, x_3, x_4\} \in V$ and $\alpha \in F$ by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^3, x_3\alpha, x_4\alpha^3\}.$$

$\Diamond$

4.4 Reconstructing near-vector spaces from fibration graphs

In this section we will see that given a fibration graph we can reconstruct an associated near-vector space.

Suppose (V, F) is a near-vector space and it is given that

$$\Gamma_{\mathcal{F}}(V) = \bigcup_{i=1}^{t} K_\alpha,$$

where $\alpha = p^r - 1$, for p a prime, $r \in \mathbb{Z}^+$. It is clear by how the graph is defined, that V would be regular. Furthermore, t gives us $|P(V)| = \dfrac{p^{rm} - 1}{p - 1}$, which in turn, gives us m. By Theorem 2.2.46, we also know that our automorphisms ψ_i's are such that $\psi_i(\alpha) = \psi_j(\alpha^{p^l})$, for $l \in \{0, \ldots, r - 1\}$. We can therefore deduce that

$$(V, F) = ((GF(p^r))^m, GF(p^r)).$$

Let us consider the case where V is non-regular, and we are given the fibration graph $\Gamma_{\mathcal{F}}(V)$ where $\Gamma_{\mathcal{F}}(V) = \Gamma_{\mathcal{F}_1}(V_1) \cup \cdots \cup \Gamma_{\mathcal{F}_l}(V_l)$ and for $t_i = |P(V_i)|$,

$$\Gamma_{\mathcal{F}_i}(V_i) = \bigcup_{j=1}^{t_i} K_\alpha, \quad i \in \{1, \ldots, l\}, \text{ where } \alpha = p^r - 1.$$

Then we proceed with the following steps:

1. Given α, we have that $\alpha + 1 = p^r$, hence, $F = GF(p^r)$.
2. Given t_i, we have that $|P(V_i)| = \dfrac{p^{rm_i} - 1}{p - 1} = t_i$, for $i = \{1, \ldots, l\}$. Hence, for all $i = \{1, \ldots, l\}$ we can calculate m_i.
3. Let $V = F^m$ with $m = m_1 + m_2 + \ldots + m_l$.
4. Construct a partition $A_1, A_2, \ldots, A_l$ of m with $|A_i| = l$, where $i \in \{1, 2, \ldots, l\}$.
5. Next, construct a suitable sequence $(s_1, \ldots, s_l)$ where $s_1 \leq s_2 \leq \cdots \leq s_l$.
6. Define the scalar multiplication for all $(x_1, x_2, x_3, x_4\} \in V$ and $\alpha \in F$ by

$$(x_1, x_2, \ldots, x_m)\alpha = (x_1\alpha^{g_1}, x_2\alpha^{g_2}, \ldots, x_m\alpha^{g_m}),$$

   where $\alpha^{g_j} = \alpha^{s_i}$ for $j \in A_i$, $i = 1, 2, \ldots, l$ and $j \in \{1, 2, \ldots m\}$.
7. Then (V, F) is a near-vector space with fibration graph $\Gamma_{\mathcal{F}}(V)$. If we chose a different partition of $\{1, 2, \ldots, m\}$, then we will get a different near-vector space, not necessarily isomorphic to the first.

The following example will illustrate the above algorithm.

Example 4.4.1.
Suppose we are given the following graphs:

$$\Gamma_{\mathcal{F}_1}(V_1) = \bigcup_{i=1}^{13} K_{26},$$

$$\Gamma_{\mathcal{F}_2}(V_2) = \bigcup_{i=1}^{364} K_{26}$$

$$\Gamma_{\mathcal{F}_3}(V_3) = \bigcup_{i=1}^{13} K_{26}$$

where $\Gamma_{\mathcal{F}}(V) = \Gamma_{\mathcal{F}_1}(V_1) \cup \Gamma_{\mathcal{F}_2}(V_2) \cup \Gamma_{\mathcal{F}_3}(V_3)$. *By Theorem 3.2.30, we have that* (V, F) *is not a regular near-vector space, where the canonical decomposition of* V *is given, in this instance, by* $V = V_1 \oplus V_2 \oplus V_3$. *Then,*

1. *Let* $\alpha = 27$ *and* $F = GF(3^3)$.
2. *Since* $|P(V_1)| = 13 = |P(V_3)|$ *and* $|P(V_2)| = 364$, *we have that* $m_1 = m_3 = 1$ *and* $m_2 = 2$.
3. *Then* $m = 4$ *and* $V = (GF(3^3))^4$.
4. *We can choose a partition of* $\{1, \ldots, m\}$, *say* A_1, A_2 *and* A_3 *where* $A_1 = \{1\}$, $A_2 = \{2, 3\}$ *and* $A_3 = \{4\}$.
5. *Choose a suitable sequence, say* $\{1, 5, 5, 7\}$.
6. *Define the scalar multiplication for all* $(x_1, x_2, x_3, x_4\} \in V$ *and* $\alpha \in F$ *by*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^5, x_3\alpha^5, x_4\alpha^7).$$

7. *Then* (V, F) *is a possible near-vector space with fibration graph* $\Gamma_{\mathcal{F}}(V) = \Gamma_{\mathcal{F}_1}(V_1) \cup \Gamma_{\mathcal{F}_2}(V_2) \cup \Gamma_{\mathcal{F}_3}(V_3)$.

◊

4.5 Reconstructing a Dickson near-field from a given graph

The final reconstruction we look at is that of a finite Dickson near-field from a graph with a particular number of vertices and involutions. We first give the definition of an involution, as well as where these are found in a finite Dickson near-field.

Definition 4.5.1. *An element in a group that is its own inverse is called an involution.*

By Lemma 2.1.15, since $(H, \circ_\phi)$ is a group, it will contain the multiplicative inverses of its elements. Moreover, $(H, \circ_\phi)$ is a normal subgroup of $(DF(q,n)^*, \circ_\phi)$ (see [26]), and so the cosets of H in $DF(q,n)^*$ form a group under $\circ_\phi$.

For the results that follow in this section, we will use the following property: for Dickson pairs (q,n) where $n|(q-1)$ we have that for $v, w \in \{0,1,\ldots,n-1\}$:

$$H\beta^v \circ_\phi H\beta^w = H\beta^u \text{ if and only if } (v+w) \equiv u \bmod n.$$

We include a proof in Appendix B. It is known that the coset H is a normal subgroup of the multiplicative elements of the Dickson near-field, $\mathrm{DF}(q,n)^*$ under $\circ_\phi$ and the cosets of H in $(\mathrm{DF}(q,n)^*, \circ_\phi)$ form a commutative group under $\circ_\phi$(see for example, [31]). It is interesting to note that if n is even, there is one other coset with the property of containing its own inverses.

Proposition 4.5.2. *For the Dickson near-field $(DF(q,n)^*, \circ_\phi)$ where n is even and $n|(q-1)$, $H\beta^{\frac{n}{2}}$ is the only other coset besides H that contains its own inverses.*

Proof. Since n is even, there exists an $s \in \{0,1,\ldots,n-1\}$ such that $s = \frac{n}{2}$ and since $2s \equiv 0 \pmod n$, we have that,

$$H\beta^s \circ_\phi H\beta^s = H \text{ if and only if } 2s \equiv 0 \bmod n.$$

Also, since $n|(q-1)$ we have that $q-1$ is even. By Theorem 2.1.14, $q-1$ divides the order of the group $(H,\cdot)$. This implies that all the cosets have even order, and in particular, $H\beta^s$. Since the product of any two elements in $H\beta^s$ is an element of H and $1 \in H$, it follows that for each element $x \in H\beta^s$, there exists an element $y \in H\beta^s$ such that $x \circ_\phi y \equiv 1 \bmod (q^n-1)$. Hence, $H\beta^s$ contains its own multiplicative inverses.
Suppose there is another coset than contains its own inverses. This would imply that for some $0 < t < n-1$, we have

$$H\beta^t \circ_\phi H\beta^t = H \text{ if and only if } 2t \equiv 0 \bmod n.$$

Then,

$$2s \equiv 2t \bmod n,$$

but both $0 < s, t < n-1$ so $s = t$. □

Proposition 4.5.3. *For $(DF(q,n)^*, \circ_\phi)$ where $n|(q-1)$, if the order of H is even then H contains two involutions, namely 1 and $\beta^{\frac{q^n-1}{2}}$. On the other hand, if the order of H is odd, then 1 is the only involution. H contains the only involutions.*

Proof. Suppose H has even order. Since $1 \in H$ and it is an involution, there exists at least one more element in H that is its own inverse. This follows from the fact that H is a group and inverses are unique. Suppose $x \in H$ is an involution other than 1, then $x = \beta^{tn}$ for some $t \in \mathbb{Z}$. Then, since x is an involution,

$$\beta^{tn} \circ_\phi \beta^{tn} = \beta^{2tn} = 1.$$

Therefore,

$$\begin{aligned} 2tn &\equiv q^n - 1 \bmod (q^n - 1) \\ t &\equiv \frac{q^n - 1}{2n} \bmod (q^n - 1). \end{aligned}$$

Since t is half of the number of elements in the coset, we will only ever have one value for t modulo $q^n - 1$. Therefore the other, and only other, involution in H has the form $x = \beta^{\frac{q^n-1}{2}}$. If the order of H is odd, and since H is a group, we have that 1 is the only involution in H.
Suppose there exists another coset other than H that contains involutions. Then this is only possible if the coset in question contains its own inverses. By Proposition 4.5.2, this coset is $H\beta^s$ where $s = \dfrac{n}{2}$ and n is even. Let us suppose that the element $\beta^{nk+s} \in H\beta^s$, $s = \dfrac{n}{2}$, is an involution. Then we have that

$$\begin{aligned} (\beta^{nk+s})^{q^s}\beta^{nk+s} &= (\beta^{nk+s})^{q^s+1} \bmod (q^n - 1) \\ &= \beta^{q^n-1} \bmod (q^n - 1) \end{aligned}$$

We want to show that H contains the only involutions. Therefore the element β^{nk+s} can only be in H, which means that $s = 0$. If we look at the powers of β only, we have modulo $q^n - 1$:

$$(nk+s)(q^s+1) = q^n - 1 = (q^{\frac{n}{2}} - 1)(q^{\frac{n}{2}} + 1).$$

So

$$nk + s = q^{\frac{n}{2}} - 1,$$

but $n|(q-1)$ and therefore $n|(q^{\frac{n}{2}} - 1)$. Hence, $s = 0$ and the only elements that are involutions are of the form β^{nk}, which are the elements of H. □

The following theorem answers the question of whether we can construct a finite near-field given a graph G.

Theorem 4.5.4. *For a given graph G of order $q^n - 1$ where (q, n) is a pair of Dickson numbers such that $q^n - 1$ is odd, let G have*

(a) one universal vertex; and

(b) $q^n - 2$ vertices of degree $q^n - 3$.

Then there exists a finite near-field F isomorphic to a finite Dickson near-field $DF(q, n)$ such that $(DF(q, n)^*, \circ_\phi)$ has cardinality $q^n - 1$ and one involution.

Proof. Suppose G is a graph of odd order $q^n - 1$ that has one universal vertex, and $q^n - 2$ vertices of degree $q^n - 3$.

Since (q, n) is a pair of Dickson numbers, by Theorem 2.1.11, we can construct a finite Dickson near-field $\mathrm{DF}(q, n)$ with order q^n, generator β, and n cosets $\{H, H\beta, \ldots, H\beta^{n-1}\}$. Let $V(G) = \{1, \ldots, q^n - 1\}$ denote the vertex set of G where $q^n - 1$ is the universal vertex of G. From now on, we will use the notation (s) to denote the vertex corresponding to the label $s \in \{1, \ldots, q^n - 1\}$. Define

$$\begin{aligned} \theta : V(G) &\to \mathrm{DF}(q, n) \\ h &:\mapsto \beta^h, \qquad h \in \{1, \ldots, q^n - 1\} \end{aligned}$$

Note that $\theta(q^n - 1) = \beta^{q^n - 1} = 1$.
Then we can construct a finite near-field $(F, +, *)$ that is isomorphic to the finite Dickson near-field $(DF(q, n), +, \circ_\phi)$ as follows. For all $i, j \in V(G)$, let

$$i * j = \begin{cases} (\theta(i) \circ_\phi \theta(j)) \bmod (q^n - 1) & \text{if } \ ij \in E(G) \text{ or } \ i = j \\ 1 & \text{otherwise} \end{cases}$$

and addition is defined in the normal way, modulo q^n.

Let $F = \{\theta(i) | i \in \{1, \ldots, q^n - 1\}\}$. We will prove that $(F, +, *)$ is a finite near-field:

(a) $(F, +)$ is a group;

(b) $(F, *)$ is a semigroup:

Suppose i, j and $k \in V(G)$, then for $ij, jk \in E(G)$,

$$\begin{aligned} (i * j) * k &= \theta(i * j) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1). \end{aligned}$$

Without loss of generality, suppose that $i \in H\beta^s, j \in H\beta^t, k \in H\beta^w$. Then

$$\begin{aligned}
(i*j)*k &= ((\beta^i)^{q^t}\beta^j) \circ_\phi \beta^k \bmod (q^n-1) \\
&= ((\beta^i)^{q^t}\beta^j)^{q^w} \cdot \beta^k \bmod (q^n-1) \\
&= (\beta^i)^{q^{t+w}}(\beta^j)^{q^w}\beta^k \bmod (q^n-1) \\
&= (\beta^i)^{q^{t+w}}(\beta^j \circ_\phi \beta^k) \bmod (q^n-1) \\
&= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\
&= i*(j*k).
\end{aligned}$$

If $ij \notin E(G)$ and $jk \in E(G)$, then

$$\begin{aligned}
(i*j)*k &= 1 \circ_\phi \theta(k) \bmod (q^n-1) \\
&= 1^{q^w}\beta^k \bmod (q^n-1) \\
&= \beta^k \\
&= \theta(k)
\end{aligned}$$

and

$$\begin{aligned}
i*(j*k) &= \beta^i \circ_\phi (\beta^j)^{q^w}\beta^k \bmod (q^n-1) \\
&= (\beta^i)^{q^{t+w}}(\beta^j)^{q^w}\beta^k \bmod (q^n-1) \\
&= ((\beta^i)^{q^t}\beta^j)^{q^w}\beta^k \bmod (q^n-1) \\
&= 1 \cdot \beta^k \bmod (q^n-1) \\
&= \theta(k).
\end{aligned}$$

Hence, $(i*j)*k = i*(j*k)$.

Alternatively, let $ij \in E(G)$ and $jk \notin E(G)$, then

$$\begin{aligned}(i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1)\\ &= ((\beta^i)^{q^t}\beta^j)^{q^w}\beta^k \bmod (q^n-1)\\ &= \beta^{iq^{t+w}}\beta^{jq^w+k}\\ &= \beta^{iq^{t+w}} \cdot 1\\ &= \beta^{iq^{t+w}}\end{aligned}$$

and

$$\begin{aligned}i*(j*k) &= \beta^i \circ_\phi 1 \bmod (q^n-1)\\ &= (\beta^i)^{q^{t+w}}(\beta^j)^{q^w}\beta^k \bmod (q^n-1)\\ &= (\beta^i)^{q^{t+w}} \cdot 1 \bmod (q^n-1)\\ &= \beta^{iq^{t+w}}.\end{aligned}$$

Therefore, $(i*j)*k = i*(j*k)$. Since all but one vertex have degree q^n-3 we cannot have that both ij and jk are not in the edge set, $E(G)$. Finally, we have to consider when $(i*j)k \notin E(G)$ where $i(j*k) \in E(G)$, and $i(j*k) \notin E(G)$ where $(i*j)k \in E(G)$.

Suppose $(i*j)k \notin E(G)$ and $i(j*k) \in E(G)$. Then we have will have two cases.

Case 1: If both $i*j \in H$ and $k \in H$:

(i) Let $i, j \in H$, then

$$\begin{aligned}(i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1)\\ &= (\beta^i\beta^j)\beta^k \bmod (q^n-1)\\ &= \beta^{i+j+k}\\ &= 1,\end{aligned}$$

where $(i+j)+k \equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned} i*(j*k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\ &= (\beta^i)(\beta^j\beta^k) \bmod (q^n-1) \\ &= \beta^{i+j+k} \\ &= 1, \end{aligned}$$

since $i+j+k \equiv 0 \bmod (q^n-1)$. Hence, $(i*j)*k = i*(j*k)$.

(ii) Let $i \in H\beta^s$ and $j \in H\beta^t$ such that $H\beta^s \circ_\phi H\beta^t = H$, then

$$\begin{aligned} (i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1) \\ &= ((\beta^i)^{q^t}\beta^j)\beta^k \bmod (q^n-1) \\ &= \beta^{iq^t+j+k} \\ &= 1, \end{aligned}$$

where $(iq^t+j)+k \equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned} i*(j*k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\ &= (\beta^i)^{q^t}(\beta^j\beta^k) \bmod (q^n-1) \\ &= \beta^{iq^t+j+k}. \\ &= 1, \end{aligned}$$

since $iq^t+j+k \equiv 0 \bmod n$. Hence, $(i*j)*k = i*(j*k)$. Since coset multiplication in $(DF(q,n)^*, \circ_\phi)$ under $\circ_\phi$ is commutative, we don't need to verify result for $i \in H\beta^t$ and $j \in H\beta^s$

Case 2: If $(i*j) \in H\beta^s$ and $k \in H\beta^t$, where $H\beta^s \circ \phi H\beta^t = H$ where $s+t \equiv 0 \bmod n$:

(i) Let $i \in H$ and $j \in H\beta^s$, then

$$\begin{aligned}(i * j) * k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= ((\beta^i)^{q^s} \beta^j)^{q^t} \beta^k \bmod (q^n - 1) \\ &= \beta^{(iq^s + j)q^t + k} \\ &= \beta^{(i + jq^t) + k} \\ &= 1,\end{aligned}$$

where $(i + jq^t) + k \equiv 0 \bmod (q^n - 1)$ and

$$\begin{aligned}i * (j * k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= (\beta^i)^{q^{s+t}} ((\beta^j)^{q^t} \beta^k) \bmod (q^n - 1) \\ &= \beta^{iq^s q^t + jq^t + k} \\ &= \beta^{(i + jq^t) + k} \\ &= 1,\end{aligned}$$

since $(i + jq^t) + k \equiv 0 \bmod (q^n - 1)$. Hence, $(i * j) * k = i * (j * k)$. Since coset multiplication in $(DF(q, n)^*, \circ_\phi)$ under $\circ_\phi$ is commutative, we don't need to verify result for $i \in H\beta^s$ and $j \in H$.

(ii) Let $i \in H\beta^a$ and $j \in H\beta^b$ such that $H\beta^a \circ_\phi H\beta^b = H\beta^s$ where $a + b \equiv s \bmod n$, then

$$\begin{aligned}(i * j) * k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= ((\beta^i)^{q^b} \beta^j)^{q^t} \beta^k \bmod (q^n - 1) \\ &= \beta^{(iq^b + j)q^t + k} \\ &= 1,\end{aligned}$$

where $[(iq^b + j)q^t] + k \equiv 0 \bmod (q^n - 1)$ and

$$\begin{aligned} i * (j * k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= (\beta^i)^{q^{b+t}}((\beta^j)^{q^t}\beta^k) \bmod (q^n - 1) \\ &= \beta^{iq^bq^t + jq^t + k} \\ &= \beta^{(iq^b+j)q^t+k} \\ &= 1, \end{aligned}$$

since $[(iq^b + j)q^t] + k \equiv 0 \bmod (q^n - 1)$. Hence, $(i * j) * k = i * (j * k)$.

We now look at if $i(j*k) \notin E(G)$ but $(i*j)k \in E(G)$. Again, we will have two cases.

Case 1: If both $i \in H$ and $j * k \in H$:

(i) Let $j, k \in H$, then

$$\begin{aligned} i * (j * k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= \beta^i(\beta^j\beta^k) \\ &= \beta^{i+(j+k)} \\ &= 1, \end{aligned}$$

where $i + (j + k) \equiv 0 \bmod (q^n - 1)$, and

$$\begin{aligned} (i * j) * k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= (\beta^i\beta^j)\beta^k \bmod (q^n - 1) \\ &= \beta^{(i+j)+k} \\ &= 1, \end{aligned}$$

since $(i + j) + k \equiv 0 \bmod (q^n - 1)$. Hence, $i * (j * k) = (i * j) * k$.

(ii) Let $j \in H\beta^s$ and $k \in H\beta^t$ such that $H\beta^s \circ_\phi H\beta^t = H$ where $s+t \equiv 0 \bmod n$, then

$$\begin{aligned} i*(j*k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\ &= (\beta^i)((\beta^j)^{q^t}\beta^k) \bmod (q^n-1) \\ &= \beta^{i+jq^t+k} \\ &= 1, \end{aligned}$$

where $(i+jq^t)+k \equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned} (i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1) \\ &= ((\beta^i)^{q^s}\beta^j)^{q^t}\beta^k \bmod (q^n-1) \\ &= \beta^{iq^{s+t}+jq^t+k} \\ &= \beta^{i+jq^t+k} \\ &= 1, \end{aligned}$$

since $i+jq^t+k \equiv 0 \bmod n$. Hence, $i*(j*k) = (i*j)*k$.

Case 2: If $i \in H\beta^s$ and $(j*k) \in H\beta^t$ such that $H\beta^s \circ \phi H\beta^t = H$, where $s+t \equiv 0 \bmod n$:

(i) Let $j \in H$ and $k \in H\beta^t$, then

$$\begin{aligned} i*(j*k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\ &= (\beta^i)^{q^t}((\beta^j)^{q^t}\beta^k) \bmod (q^n-1) \\ &= \beta^{iq^t+jq^t+k} \\ &= \beta^{(i+j)q^t+k} \\ &= 1, \end{aligned}$$

where $[(i+j)q^t]+k \equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned}(i*j)*k &= (\theta(i)\circ_\phi \theta(j))\circ_\phi \theta(k) \bmod (q^n-1)\\ &= (\beta^i\beta^j)^{q^t}\beta^k \bmod (q^n-1)\\ &= \beta^{(i+j)q^t+k}\\ &= 1,\end{aligned}$$

since $[(i+j)q^t]+k \equiv 0 \bmod (q^n-1)$. Hence, $i*(j*k)=(i*j)*k$. Since coset multiplication in $(DF(q,n)^*,\circ_\phi)$ under $\circ_\phi$ is commutative, we don't need to verify result for $j \in H\beta^t$ and $k \in H$.

(ii) Let $i \in H\beta^a$ and $j \in H\beta^b$ such that $H\beta^a \circ_\phi H\beta^b = H\beta^s$ where $a+b \equiv s \bmod n$, then

$$\begin{aligned}i*(j*k) &= \theta(i)\circ_\phi(\theta(j)\circ_\phi\theta(k)) \bmod (q^n-1)\\ &= (\beta^i)^{q^t}((\beta^j)^{q^b}\beta^k) \bmod (q^n-1)\\ &= \beta^{iq^t+(jq^b+k)}\\ &= 1,\end{aligned}$$

where $iq^t+(jq^b+k) \equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned}(i*j)*k &= (\theta(i)\circ_\phi \theta(j))\circ_\phi \theta(k) \bmod (q^n-1)\\ &= ((\beta^i)^{q^a}\beta^j)^{q^b}\beta^k \bmod (q^n-1)\\ &= \beta^{(iq^{a+b}+jq^b+k}\\ &= \beta^{(iq^t+(jq^b+k)}\\ &= 1,\end{aligned}$$

since $iq^t+(jq^b+k) \equiv 0 \bmod (q^n-1)$. Hence, $i*(j*k)=(i*j)*k$.

Once again, since all but one vertex have degree q^n-3 we cannot have that both $(i*j)k$ and $i(j*k)$ are not in the edge set, $E(G)$.

(c) For $i, j, k \in V(G)$, $k \in H\beta^w$ and $ij, jk \in E(G)$,

$$\begin{aligned}(i+j) * k \bmod (q^n-1) &= \theta(i+j) \circ_\phi \theta(k) \bmod (q^n-1) \\ &= (\beta^{(i+j)})^{q^w}\beta^k \bmod (q^n-1) \\ &= ((\beta^i)^{q^w} + (\beta^j)^{q^w})\beta^k \bmod (q^n-1) \\ &= ((\beta^i)^{q^w}\beta^k + (\beta^j)^{q^w}\beta^k) \bmod (q^n-1) \\ &= (\theta(i) \circ_\phi \theta(k)) + (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\ &= (i * k) + (j * k) \bmod (q^n-1).\end{aligned}$$

(d) Since (q^n-1) has degree q^n-2, we have that it is adjacent to all other vertices. For all $i \in V(G)$,

$$\begin{aligned}(i * (q^n-1)) \bmod (q^n-1) &= (\theta(i) \circ_\phi \theta(q^n-1)) \bmod (q^n-1) \\ &= \beta^i \circ_\phi \beta^{q^n-1} \bmod (q^n-1) \\ &= \beta^i \bmod (q^n-1) \\ &= \theta(i) \bmod (q^n-1) \\ &= (\beta^{q^n-1} \circ_\phi \beta^i) \bmod (q^n-1) \\ &= (\theta(q^n-1) \circ_\phi \theta(i)) \bmod (q^n-1) \\ &= ((q^n-1) * i) \bmod (q^n-1).\end{aligned}$$

Hence q^n-1 is the identity element of $(F, *)$.

(e) For all $i \in V(G)$ such that $(i) \neq (q^n-1)$, there exists a unique vertex (j) such that $ij \notin E(G)$. However, for $i \in H\beta^s$ and $j \in H\beta^t$ if and only if $s+t \equiv 0 \pmod{n}$ and $s, t \in \{0, 1, \ldots, n-1\}$, therefore:

$$\begin{aligned}(i * j) &= (\theta(i) \circ_\phi \theta(j)) \bmod (q^n-1) \\ &= 1 \bmod (q^n-1) \\ &= (\theta(j) \circ_\phi \theta(i)) \bmod (q^n-1) \\ &= (j * i).\end{aligned}$$

Since 1 is a universal vertex in the graph, it is its own inverse, it follows that 1 is an involution. Therefore every element in F has a unique inverse. Hence, $(F, +, *)$ is a finite near-field and it is isomorphic to $(DF(q,n), +, \circ_\phi)$.

□

Theorem 4.5.5. *For a given graph G of order $q^n - 1$ where (q, n) is a pair of Dickson numbers such that $q^n - 1$ is even, let*

(a) G have two universal vertices; and

(b) $(q^n - 3)$ vertices have degree $(q^n - 3)$.

Then there exists a finite near-field F isomorphic to a finite Dickson near-field $DF(q,n)$ such that $(DF(q,n)^*, \circ_\phi)$ has cardinality $q^n - 1$ and two involutions.

Proof. Suppose G is a graph of even order $q^n - 1$ that has two universal vertices, and $q^n - 3$ vertices of degree $q^n - 3$.

Then we can construct a finite near-field $(F, +, *)$ that is isomorphic to the finite Dickson near-field $(DF(q,n), +, \circ_\phi)$ in a similar way as we did in Theorem 4.5.4. Let $V(G) = \{1, \ldots, q^n - 1\}$ denote the vertex set of G where $q^n - 1$ is one of the universal vertices of G. We again define

$$\begin{aligned} \theta : V(G) &\to \mathrm{DF}\ (q,n) \\ h &:\mapsto \beta^h, \qquad h \in \{1, \ldots, q^n - 1\} \end{aligned}$$

Note that $\theta(q^n - 1) = \beta^{q^n - 1} = 1$.
For all $i, j \in V(G)$, let

$$i * j = \begin{cases} (\theta(i) \circ_\phi \theta(j)) \bmod (q^n - 1) & \text{if } ij \in E(G) \text{ or } \text{if } i = j \\ 1 & \text{otherwise} \end{cases}$$

and addition is defined in the normal way, modulo q^n.

Let $F = \{\theta(i) | i \in \{1, \ldots, q^n - 1\}\}$. Then as in the previous theorem, all the verifications of the axioms except for the one for associativity will be the same. Note that for $q^n - 1$ even, we could have that n is either even or odd. For n odd, our verification would be similar to the previous theorem. We will show for n even, that

(b) $(F, *)$ is a semigroup:
Suppose i, j and $k \in V(G)$, then for $ij, jk \in E(G)$,

$$\begin{aligned}(i * j) * k &= \theta(i * j) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1).\end{aligned}$$

Without loss of generality, suppose that $i \in H\beta^s, j \in H\beta^t, k \in H\beta^w$. Then

$$\begin{aligned}(i * j) * k &= ((\beta^i)^{q^t}\beta^j) \circ_\phi \beta^k \bmod (q^n - 1) \\ &= ((\beta^i)^{q^t}\beta^j)^{q^w} \cdot \beta^k \bmod (q^n - 1) \\ &= (\beta^i)^{q^{t+w}}(\beta^j)^{q^w}\beta^k \bmod (q^n - 1) \\ &= (\beta^i)^{q^{t+w}}(\beta^j \circ_\phi \beta^k) \bmod (q^n - 1) \\ &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= i * (j * k).\end{aligned}$$

If $ij \notin E(G)$ and $jk \in E(G)$, then

$$\begin{aligned}(i * j) * k &= 1 \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= 1^{q^w}\beta^k \bmod (q^n - 1) \\ &= \beta^k \\ &= \theta(k)\end{aligned}$$

and

$$\begin{aligned}i * (j * k) &= \beta^i \circ_\phi (\beta^j)^{q^w}\beta^k \bmod (q^n - 1) \\ &= (\beta^i)^{q^{t+w}}(\beta^j)^{q^w}\beta^k \bmod (q^n - 1) \\ &= ((\beta^i)^{q^t}\beta^j)^{q^w}\beta^k \bmod (q^n - 1) \\ &= 1 \cdot \beta^k \bmod (q^n - 1) \\ &= \theta(k).\end{aligned}$$

Hence, $(i * j) * k = i * (j * k)$.

Alternatively, let $ij \in E(G)$ and $jk \notin E(G)$, then

$$\begin{aligned}(i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1)\\ &= ((\beta^i)^{q^t}\beta^j)^{q^w}\beta^k \bmod (q^n-1)\\ &= \beta^{iq^{t+w}}\beta^{jq^w+k}\\ &= \beta^{iq^{t+w}} \cdot 1\\ &= \beta^{iq^{t+w}},\end{aligned}$$

and

$$\begin{aligned}i*(j*k) &= \beta^i \circ_\phi 1 \bmod (q^n-1)\\ &= (\beta^i)^{q^{t+w}}(\beta^j)^{q^w}\beta^k \bmod (q^n-1)\\ &= (\beta^i)^{q^{t+w}} \cdot 1 \bmod (q^n-1)\\ &= \beta^{iq^{t+w}}.\end{aligned}$$

Therefore, $(i*j)*k = i*(j*k)$.
Since all but two vertices have degree q^n-3 we cannot have that both ij and jk are not in the edge set, $E(G)$.
We now consider the different cases for n even when $(i*j)k \notin E(G)$ where $i(j*k) \in E(G)$, and $i(j*k) \notin E(G)$ where $(i*j)k \in E(G)$.

Suppose $(i*j)k \notin E(G)$ and $i(j*k) \in E(G)$. Then we have three cases. We note that coset multiplication in $(DF(q,n)^*, \circ_\phi)$ under $\circ_\phi$ is commutative.

Case 1: If both $i*j \in H$ and $k \in H$:

(i) Let $i, j \in H$, then

$$\begin{aligned}(i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1)\\ &= (\beta^i\beta^j)\beta^k \bmod (q^n-1)\\ &= \beta^{i+j+k}\\ &= 1,\end{aligned}$$

where $(i+j)+k \equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned} i*(j*k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\ &= (\beta^i)(\beta^j\beta^k) \bmod (q^n-1) \\ &= \beta^{i+j+k} \\ &= 1, \end{aligned}$$

since $i+j+k \equiv 0 \bmod (q^n-1)$. Hence, $(i*j)*k = i*(j*k)$.

(ii) Let $i \in H\beta^s$ and $j \in H\beta^t$ such that $H\beta^s \circ_\phi H\beta^t = H$, then

$$\begin{aligned} (i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1) \\ &= ((\beta^i)^{q^t}\beta^j)\beta^k \bmod (q^n-1) \\ &= \beta^{iq^t+j+k} \\ &= 1, \end{aligned}$$

where $(iq^t+j)+k \equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned} i*(j*k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n-1) \\ &= (\beta^i)^{q^t}(\beta^j\beta^k) \bmod (q^n-1) \\ &= \beta^{iq^t+j+k}. \\ &= 1, \end{aligned}$$

since $iq^t+j+k \equiv 0 \bmod n$. Hence, $(i*j)*k = i*(j*k)$.

(iii) Let $i,j \in H\beta^{\frac{n}{2}}$ and let $s' = \frac{n}{2}$, then

$$\begin{aligned} (i*j)*k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n-1) \\ &= ((\beta^i)^{q^{s'}}\beta^j)\beta^k \bmod (q^n-1) \\ &= \beta^{iq^{s'}+j+k} \\ &= 1, \end{aligned}$$

where $(iq^{s'} + j) + k \equiv 0 \bmod (q^n - 1)$ and

$$\begin{aligned} i * (j * k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= (\beta^i)^{q^{s'}} (\beta^j \beta^k) \bmod (q^n - 1) \\ &= \beta^{iq^{s'} + j + k}. \\ &= 1, \end{aligned}$$

since $(iq^{s'} + j) + k \equiv 0 \bmod n$. Hence, $(i * j) * k = i * (j * k)$.

Case 2: If $i \in H\beta^s$ and $(j * k) \in H\beta^t$ such that $H\beta^s \circ \phi H\beta^t = H$, where $s + t \equiv 0 \bmod n$:

(i) Let $i \in H$ and $j \in H\beta^s$, then

$$\begin{aligned} (i * j) * k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= ((\beta^i)^{q^s} \beta^j)^{q^t} \beta^k \bmod (q^n - 1) \\ &= \beta^{i + jq^t + k} \\ &= 1, \end{aligned}$$

where $(i + jq^t) + k \equiv 0 \bmod (q^n - 1)$ and

$$\begin{aligned} i * (j * k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= (\beta^i)((\beta^j)^{q^t} \beta^k) \bmod (q^n - 1) \\ &= \beta^{i + jq^t + k} \\ &= 1, \end{aligned}$$

since $(i + jq^t) + k \equiv 0 \bmod (q^n - 1)$. Hence, $(i * j) * k = i * (j * k)$.

(ii) Let $i \in H\beta^a$ and $j \in H\beta^b$ such that $H\beta^a \circ_\phi H\beta^b = H\beta^s$ where $a + b \equiv s \bmod n$:

$$\begin{aligned} (i * j) * k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= ((\beta^i)^{q^b} \beta^j)^{q^t} \beta^k \bmod (q^n - 1) \\ &= \beta^{iq^{b+t} + jq^t + k} \\ &= 1, \end{aligned}$$

where $(iq^{b+t} + jq^t) + k \equiv 0 \bmod (q^n - 1)$ and

$$\begin{aligned} i * (j * k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= (\beta^i)^{q^{b+t}}((\beta^j)^{q^t}\beta^k) \bmod (q^n - 1) \\ &= \beta^{iq^{b+t}+jq^b+k} \\ &= 1, \end{aligned}$$

since $(iq^{b+t} + jq^t) + k \equiv 0 \bmod (q^n - 1)$. Hence, $(i * j) * k = i * (j * k)$.

Case 3: If both $(i * j),\ k \in H\beta^{\frac{n}{2}}$, where $s' = \frac{n}{2}$:

(i) Let $i \in H$ and $j \in H\beta^{s'}$, then

$$\begin{aligned} (i * j) * k &= (\theta(i) \circ_\phi \theta(j)) \circ_\phi \theta(k) \bmod (q^n - 1) \\ &= ((\beta^i)^{q^{s'}}\beta^j)^{q^{s'}}\beta^k \bmod (q^n - 1) \\ &= \beta^{i+jq^{s'}+k} \\ &= 1, \end{aligned}$$

where $(i + jq^{s'}) + k \equiv 0 \bmod (q^n - 1)$ and

$$\begin{aligned} i * (j * k) &= \theta(i) \circ_\phi (\theta(j) \circ_\phi \theta(k)) \bmod (q^n - 1) \\ &= (\beta^i)((\beta^j)^{q^{s'}}\beta^k) \bmod (q^n - 1) \\ &= \beta^{i+jq^{s'}+k} \\ &= \beta^{(i+jq^{s'})+k} \\ &= 1, \end{aligned}$$

since $(i + jq^{s'}) + k \equiv 0 \bmod (q^n - 1)$. Hence, $(i * j) * k = i * (j * k)$.

(ii) Let $i \in H\beta^a$ and $j \in H\beta^b$ such that $H\beta^a \circ_\phi H\beta^b = H\beta^{s'}$ where $a+b \equiv s' \bmod n$:

$$\begin{aligned}(i*j)*k &= (\theta(i)\circ_\phi\theta(j))\circ_\phi\theta(k) \bmod (q^n-1)\\ &= ((\beta^i)^{q^b}\beta^j)^{q^{s'}}\beta^k \bmod (q^n-1)\\ &= \beta^{(iq^{b+s'}+jq^{s'}+k}\\ &= 1,\end{aligned}$$

where $(iq^{b+s'}+jq^{s'})+k\equiv 0 \bmod (q^n-1)$ and

$$\begin{aligned}i*(j*k) &= \theta(i)\circ_\phi(\theta(j)\circ_\phi\theta(k)) \bmod (q^n-1)\\ &= (\beta^i)^{q^{b+s'}}((\beta^j)^{q^{s'}}\beta^k) \bmod (q^n-1)\\ &= \beta^{iq^{b+s'}+jq^{s'}+k}\\ &= 1,\end{aligned}$$

since $(iq^{b+s'}+jq^{s'})+k\equiv 0 \bmod (q^n-1)$. Hence, $(i*j)*k = i*(j*k)$.

In a similar manner, we can show that multiplication is associative when $i(j*k)\notin E(G)$ where $(i*j)k\in E(G)$. Since all but two vertices have degree q^n-3 we cannot have that both $i(j*k)$ and $(i*j)k$ are not in the edge set, $E(G)$. $(F,+,*)$ is therefore a finite near-field.

We now focus on the two universal vertices in G. By Proposition 4.5.3, the coset H contains two involutions. This means that there are two elements in H that are their own inverses. Therefore every element in F has a unique inverse. Therefore, $(F,+,*)$ is a finite near-field and as such it is isomorphic to $(DF(q,n),+,\circ_\phi)$.

□

Chapter 5

Future work

Although Dickson near-fields were not extensively studied in this thesis, I am interested in its possible application to coding theory. My masters thesis covered the theory, examples and applications of error-correcting codes from a finite field perspective. With the possibility of a collaboration with a coding theorist, I am keen to investigate the idea of replacing finite fields with an appropriate Dickson near-field.

My interest in graph theory has also been peaked during this process.

In addition, I am interested in investigating quotient spaces formed by arbitrary subspaces of near-vector spaces, which in turn is formed by taking copies of finite fields.

Appendices

Appendix A

The Complete Set of Residues

The following was proved by P. Djagba in his thesis [11].

Claim: Let (q, n) be a Dickson pair. Then $\{[k]_q, 1 \leq k \leq n\}$ form a finite complete set of different residues modulo n.

Proof. Let $i(k) = \frac{q^k-1}{q-1}$ for $k = 1, \cdots, n$.

We would like to show that the set $\{i(1), i(2), \cdots, i(n)\}$ residues modulo n is the set $\{0, 1, \cdots, n-1\}$. It suffice to show that the set $\{\frac{q^k-1}{q-1}, 1 \leq k < n\}$ are distinct residues modulo n.

Suppose that

$$\frac{q^k-1}{q-1} \equiv \frac{q^l-1}{q-1} \mod n \quad 1 \leq k < l < n. \tag{A.1}$$

This implies that

$$\begin{aligned} &1 + q + \cdots + q^{k-1} \equiv 1 + q + \cdots + q^{l-1} \mod n \\ &\Rightarrow q^k + \cdots + q^{l-1} \equiv 0 \mod n \\ &\Rightarrow q^k(1 + \cdots + q^{l-k-1}) \equiv 0 \mod n \end{aligned}$$

By the definition of Dickson pair every prime divisor p of n divide $q-1$, so p does not divide q. It follows that gcd $(q, n) = 1$. Therefore

$$\begin{aligned} q^k(1 + \cdots + q^{l-k-1}) \equiv 0 \mod n &\Rightarrow 1 + \cdots + q^{l-k-1} \equiv 0 \mod n \\ &\Rightarrow \frac{q^{l-k}-1}{q-1} \equiv 0 \mod n. \end{aligned}$$

Assume that $\frac{q^t-1}{q-1} \equiv 0 \mod n$ for some $1 \leq t < n$. It follows that for all i,

$$\frac{q^t-1}{q-1} \equiv 0 \mod p_i^{\alpha_i}$$

where $n = \prod p_i^{\alpha_i}$ is the unique prime factorisation.

Assume without loss of generality that $n = p^m$.

We know that $q \equiv 1 \mod p$. So we can write $q = 1 + p\epsilon$ for some $\epsilon \in \mathbb{N}$.

Assuming that p^m divides $\frac{q^t-1}{q-1}$, we want to show that $n = p^m$ divides t leads to contradiction.

In fact

$$q^t = (1+p\epsilon)^t = \sum_{k=0}^{t} \vec{t}k(p\epsilon)^k.$$

Hence

$$\frac{q^t-1}{q-1} = \sum_{k=1}^{t} \vec{t}k(p\epsilon)^{k-1} = \cdots + \vec{t}2p\epsilon + t.$$

For instance

- if $m = 1$, then the assumption is

  $$p/\frac{q^t-1}{q-1} \Leftrightarrow p/\sum_{k=1}^{t} \vec{t}k(p\epsilon)^{k-1} \Leftrightarrow p/t$$

  leads to contradiction since $p = n > t$.

- if $m = 2$,

  $$p^2/\frac{q^t-1}{q-1} \Leftrightarrow p^2/\sum_{k=1}^{t} \vec{t}k(p\epsilon)^{k-1} \Leftrightarrow p/\vec{t}2p\epsilon + t \Rightarrow p/t$$

  But then $\vec{t}2 = \frac{t(t-1)}{2}$, so $p/\vec{t}2$. Hence $p^2/\vec{t}2p\epsilon$. Thus p^2/t leads to contradiction.

- By the same approach for some m, $p^m/\frac{q^t-1}{q-1} \Rightarrow n = p^m/t$ leads to contradiction.

  Therefore the assumption A.1 can not hold. Thus the set $\left\{\frac{q^k-1}{q-1}, 1 \leq k < n\right\}$ are distinct residues modulo n.

□

Appendix B

Coset multiplication modulo n for Dickson near-fields, where $n|q-1$

For a pair of Dickson numbers (q, n) such that $n|(q-1)$, the following is true for $v, w \in \{0, 1, \ldots, n-1\}$:

$$H\beta^v \circ_\phi H\beta^w = H\beta^u \text{ if and only if } u \equiv (v+w) \bmod n.$$

Proof. Suppose $u \equiv (v+w) \bmod n$. We will first show that $H\beta^v \circ_\phi H\beta^w \subseteq H\beta^u$.
Let $a \in H\beta^v$ and $b \in H\beta^w$, then $a = \beta^{nk_1+v}$ and $b = \beta^{nk_2+w}$ for integers k_1, k_2 and $v, w \in \{0, 1, \ldots, n-1\}$.
If $w = 0$ then, since $v \in \{0, 1, \ldots, n-1\}$, $u = v \bmod n$, we have that

$$\begin{aligned} a \circ_\phi b &= ab \\ &= \beta^{nk_1+v}\beta^{nk_2} \\ &= \beta^{n(k_1+k_2)+v} \in H\beta^v = H\beta^u. \end{aligned}$$

If $w \neq 0$ then, since $q = nt + 1$ for $t \in \mathbb{Z}$, we have that

$$\begin{aligned}
a \circ_\phi b &= a^{q^w} b \\
&= \left(\beta^{nk_1+v}\right)^{q^w} \beta^{nk_2+w} \\
&= \beta^{nk_1q^w+vq^w+nk_2+w} \\
&= \beta^{n(k_1q^w+k_2)+vq^w+w} \\
&= \beta^{n(k_1q^w+k_2)+v(nt+1)^w+w} \\
&= \beta^{n(k_1q^w+k_2)+v(n^wt^w+\cdots+wnt+1)+w} \\
&= \beta^{n(k_1q^w+k_2)+v(n^wt^w+\cdots+wnt)+v+w} \\
&= \beta^{n(k_1q^w+k_2)+n(vn^{w-1}t^w+\cdots+vwt)+v+w} \\
&= \beta^{n(k_1q^w+k_2+vn^{w-1}t^w+\cdots+vwt)+v+w} \\
&\in H\beta^{v+w} = H\beta^u.
\end{aligned}$$

Hence, $H\beta^v \circ_\phi H\beta^w \subseteq H\beta^u$ for $v, w \in \{0, 1, \ldots, n-1\}$ where $u \equiv (v+w) \bmod n$. For the other inclusion, suppose that $x \in H\beta^u$. Since $(\mathrm{DF}(q,n)^*, \circ_\phi)$ is a group, we know that there exists two elements, $y_1, y_2 \in \mathrm{DF}(q,n)^*$ say, such that

$$y_1 \circ_\phi y_2 = x.$$

Suppose that $y_1 \in H\beta^{s_1}$ and $y_2 \in H\beta^{s_2}$ where $s_1, s_2 \in \{0, 1, \ldots, n-1\}$.

Case 1: If $s_2 \neq 0$, then for $l_1, l_2 \in \mathbb{Z}$,

$$\begin{aligned}
y_1 \circ_\phi y_2 &= y_1^{q^{s_2}} y_2 \\
&= \left(\beta^{nl_1+s_1}\right)^{q^{s_2}} \beta^{nl_2+s_2} \\
&= \beta^{n(l_1q^{s_2}+l_2)+s_1(nt+1)^{s_2}+s_2} \\
&= \beta^{n(l_1q^{s_2}+l_2)+s_1(n^{s_2}t^{s_2}+\ldots+s_2nt)+s_1+s_2} \\
&= \beta^{n(l_1q^{s_2}+l_2)+n(s_1n^{s_2-1}t^{s_2}+\ldots+s_1s_2t)+s_1+s_2} \\
&= \beta^{n(l_1q^{s_2}+l_2+s_1n^{s_2-1}t^{s_2}+\ldots+s_1s_2t)+s_1+s_2} \\
&\in H\beta^{s_1+s_2}.
\end{aligned}$$

Since $y_1 \circ_\phi y_2 = x \in H\beta^u$ and the cosets are disjoint, we have that $s_1 + s_2 \equiv v + w \bmod n$. Since the sum of integers is not unique, one of these sums will be where $s_1 = v$ and $s_2 = w$. Therefore, $y_1 \in H\beta^v$ and $y_2 \in H\beta^w$ as one possibility, and we have that $H\beta^u \subseteq H\beta^v \circ_\phi H\beta^w$.

Case 2: If $s_2 = 0$, then $y_2 \in H$. Then

$$\begin{aligned}
y_1 \circ_\phi y_2 &= y_1 y_2 \\
&= \beta^{nl_1+s_1}\beta^{nl_2} \\
&= \beta^{n(l_1+l_2)+s_1} \in H\beta^{s_1}.
\end{aligned}$$

Since $x = y_1 \circ_\phi y_2 \in H\beta^u$, we have that $H\beta^u = H\beta^{s_1}$. Since $u \equiv (v+w) \bmod n$, this implies that both $u, s_1 \in \{0, 1, \ldots, n-1\}$ and therefore $s_1 = u$. So $s_1 \equiv (v+w) \bmod n$ and since both $v, w \in \{0, 1, \ldots, n-1\}$ we have yet again that the sum, s_1, of v and w modulo n is not unique. One of these sums would include either $v = 0$ or $w = 0$, which means $s_1 = w$ or $s_1 = v$, respectively. Say $w = 0$, then $u = s_1 = v$ and we have that $H\beta^u \subseteq H\beta^u \circ_\phi H$.

Conversely, suppose that $H\beta^v \circ_\phi H\beta^w = H\beta^u$ for $v, w \in \{0, 1, \ldots, n-1\}$. Let $a \in H\beta^v$ and $b \in H\beta^w$, then $a = \beta^{nk_1+v}$ and $b = \beta^{nk_2+w}$ for integers k_1, k_2 and $v, w \in \{0, 1, \ldots, n-1\}$. Then

$$\begin{aligned}
a \circ_\phi b &= a^{q^w} b \\
&= \left(\beta^{nk_1+v}\right)^{q^w} \beta^{nk_2+w} \\
&= \beta^{nk_1q^w+vq^w+nk_2+w} \\
&= \beta^{n(k_1q^w+k_2)+vq^w+w} \\
&= \beta^{n(k_1q^w+k_2)+v(nt+1)^w+w} \\
&= \beta^{n(k_1q^w+k_2)+v(n^wt^w+\ldots+wnt+1)+w} \\
&= \beta^{n(k_1q^w+k_2)+v(n^wt^w+\ldots+wnt)+v+w} \\
&= \beta^{n(k_1q^w+k_2)+n(vn^{w-1}t^w+\ldots+vwt)+v+w} \\
&= \beta^{n(k_1q^w+k_2+vn^{w-1}t^w+\ldots+vwt)+v+w} \\
&\in H\beta^{v+w}.
\end{aligned}$$

By our assumption, $a \circ_\phi b \in H\beta^u$ and since cosets in a Dickson near-field are disjoint, we have that $u \equiv v + w \bmod n$. □

Bibliography

[1] R. Allenby, *Rings, fields and groups*, Butterworth Heineman, 2nd ed., 1991.

[2] D. Anderson, M. Axtell, and J. Stickles, *Zero-divisor graphs in commutative rings*, Commutative Algebra: Noetherian and Non-Noetherian Perspectives, (2010), pp. 23–45.

[3] J. André, *Über parallelstrukturen. teil i: Grundbegriffe.*, Mathematische Zeitschrift, 76 (1961), pp. 85–102.

[4] J. André, *Lineare Algebra über Fastkörpern*, 1974.

[5] J. Beidleman, *On near-rings and near-ring modules*, Pennsylvania State University Dissertations Mathematics, 1964.

[6] G. Chartrand, L. Lesniak, and P. Zhang, *Graphs and Digraphs*, 2011.

[7] D. Chistyakov, K.-T. Howell, and S.-P. Sanon, *On representation theory and near-vector spaces*, Linear and Multi-Linear Algebra, 67 (2019), pp. 1495–1510.

[8] A. Das, *Subspace inclusion graph of a vector space*, Communications in Algebra, 44 (2017).

[9] ——, *Subspace sum graph of a vector space*, accepted, (2017).

[10] L. Dickson, *Definitions of a group and a field by independent postulates*, Transactions of the American Mathematical Society, 6 (2018), pp. 198–204.

[11] P. Djagba, *Near vector spaces*, Stellenbosch University Dissertations Mathematics, 2019.

[12] S. Dorfling, K.-T. Howell, and S. P. Sanon, *The decomposition of finite-dimensional near-vector spaces*, Communications in Algebra, 46 (2018), pp. 3033–3046.

[13] M. Hall, *Projective planes*, Transactions of the American Mathematical Society, 54 (1943), pp. 229–277.

[14] J. M. Harris, J. L. Hirst, and M. J. Mossinghoff, *Combinatorics and graph theory*, Undergraduate texts in mathematics, Springer, New York, 2nd ed., 2008.

[15] K.-T. Howell, *Contributions to the Theory of Near-vector spaces*, Free State University Dissertations Mathematics, 2008.

[16] ——, *On subspaces and mappings of near-vector spaces*, Communications in Algebra, 43 (2015), pp. 2524–2540.

[17] ——, *Near-vector spaces determined by finite fields and their fibrations*, Turkish Journal of Mathematics, 43 (2019), pp. 2549–2560.

[18] K.-T. Howell and S. Marques, *Toward an intuitive understanding of the structure of near-vector spaces*, (submitted).

[19] K.-T. Howell and J. Meyer, *Finite-dimensional near-vector spaces over fields of prime order*, Communications in Algebra, 38 (2010), pp. 86–93.

[20] ——, *Near-vector spaces determined by finite fields*, Journal of Algebra, 398 (2014), pp. 55–62.

[21] K.-T. Howell and S. Sanon, *Linear mappings of near-vector spaces*, Quaestiones Mathematicae, 41 (2018), pp. 493–514.

[22] ——, *Near-vector spaces constructed from near domains*, Miskolc Mathematical Notes, 19 (2018), pp. 883–897.

[23] ——, *On spanning sets and generators of near-vector spaces*, Turkish Journal of Mathematics, 42 (2018), pp. 3232–3241.

[24] H. Karzel, *Fastvektorräume, unvollständige fastkörper und ihre abgeleiteten strukturen*, Proceedings of a Conference held at Oberwolfach, (1984).

[25] H. Karzel, I. Pieper, and K. Sörensen, *Inzidenzgruppen*, Universität Hamburg, 1960.

[26] G. Pilz, *Near-rings : the theory and its applications*, North-Holland mathematics studies; 23, North-Holland, Amsterdam, 1977.

[27] K. Rodtes and W. Chomjun, *On the number of near-vector spaces determined by finite fields*, Journal of Algebra, 492 (2017), pp. 90–101.

[28] S. P. Sanon, *On counting subspaces of near-vector spaces*, Discrete Mathematics, 343 (2020), p. 111739.

[29] E. Sperner, *Affine räume mit schwacher inzidenz und zugehörige algebraische strukturen.*, Journal für die reine und angewandte Mathematik, 204 (1960), pp. 205–215.

[30] A. van der Walt, *Near-linear transformations of near-vector spaces*, Proceedings of a Conference held at Oberwolfach, (1995), pp. 189–193.

[31] H. Wahling, *Theorie der Fastkörper*, Thales monographs ; 1, Thales, Essen, 1987.